Defense Manpower Data Center

Worldwide COTS Hardware, Software, Maintenance & Integration Services II (WWHWSW II)

PERFORMANCE WORK STATEMENT

1.0 INTRODUCTION

1.1 The Defense Manpower Data Center (DMDC) has a requirement for Worldwide COTS Hardware (HW), Software (SW), Maintenance, and Integration Services for the enterprise information technology (IT) systems, including the Real-time Automated Identification System (RAPIDS), Defense Biometrics Identification System (DBIDS), the Noncombatant Tracking/Emergency Tracking Accountability System (NTS/ETAS), and the Joint Asset Movement Management System (JAMMS). Services include interaction with the Department of Defense (DoD) and other federal agencies worldwide to ensure operational effectiveness of programs and applications across the DMDC enterprise.

2.0 BACKGROUND

2.1 DMDC is part of a DoD Field Activity called the Defense Human Resources Activity (DHRA). DMDC supports major programs and initiatives within the DoD. DMDC maintains the central and authoritative source of personnel, manpower, training, and security data for the Department of Defense. The personnel data holdings, in particular, are broad in scope and date back to the early 1970's covering all Uniformed Services, all components of the Total Force (Active, Guard, Reserve, and Civilian), and all phases of the personnel life cycle (accessions through separation/retirement). The categories of data archived at DMDC represent significant data holdings and, in most cases, provide the only single source of common data on the Uniformed Services. These data support decision-making by the Office of the Under Secretary of Defense (OUSD) (Personnel and Readiness), other OSD organizations, and a wide variety of customers both within and outside the Department.

2.2 DMDC operates major programs that affect individual members of the DoD, as well as other Federal Departments and Agencies. The programs support active duty, reserve, and retired military members and their families; as well as civilian and contractor employees of the DoD. These programs include verifying military entitlements and benefits; managing the DoD ID card issuance program; providing identity management for the DoD; helping identify fraud and waste in DoD systems; conducting personnel surveys; and assisting military members and their spouses with relocations, quality of life issues and transition to civilian life.

2.3 DMDC is a geographically separated organization with personnel and facilities located in Virginia (VA), California (CA), Texas (TX) and support offices in Germany, Korea, Qatar and Kuwait. The Director of DMDC is located at DMDC's offices in Alexandria, VA.

2.4 The major components of DMDC's IT for the programs supported by this Task Order are described in the following; Appendix B, "Software Overview", and Appendix C, "DMDC/DEERS WAN Infrastructure". DMDC anticipates that components, applications and information may change before and during the performance of this Task Order.

3.0 SCOPE

3.1 The scope of this acquisition is to provide all technical and management personnel, hardware/software and ancillary components, tools and supplies, other than the currently provided Government-furnished property (GFP) and Government-furnished Equipment (GFE), to meet the requirements of this PWS.

3.2 The Department of Defense (DoD), DMDC, other Federal Agencies, and branches of the Uniformed Services require information technology (IT) and integration support from a systems integrator that can deliver leading edge and secure solutions across the DMDC enterprise.

3.3 This effort requires support for a variety of services across the DMDC enterprise and may expand as mission changes for the support services listed below:

- Worldwide Site Management Support
- Worldwide Networks and Communications Engineering Support
- Outside the Continental United States (OCONUS) Support
- COTS Hardware and Software Support
- Worldwide COTS Hardware and Software Maintenance
- Integrated Program Management System (IPMS)

A List of Acronyms and Abbreviations used in this PWS is provided in Appendix A.1.

3.4 The effort shall support DMDC infrastructure including the Defense Enrollment Eligibility Reporting System (DEERS) and other DoD and federal applications that leverage data holdings. Throughout the lifetime of the task order, DMDC portfolio anticipates assuming control and support of future databases, applications and systems that will require support.

Current operational programs include the following:

3.4.1 The Real-time Automated Personnel Identification System (RAPIDS), a distributed worldwide network of personal computers (PCs) and laptops with Common Access Card (CAC) and other Identification (ID) card production peripherals, which communicates with the DEERS database and the Defense Information Systems Agency (DISA) Certification Authorities (CAs) via Issuance Portals. For additional RAPIDS Information reference Appendix D.1 through Appendix D.9.

3.4.2 The Defense Biometric Identification System (DBIDS) uses PCs, laptops, and mobile handheld computers that are networked via wireless, local area networks (LANs), and wide area networks (WANs) to communicate with co-located local base, command-wide, and/or global DMDC database servers. For additional DBIDS Information reference Appendix E.1 through Appendix E.6.

3.4.3 The Noncombatant Evacuation Operations (NEO) Tracking System (NTS) (OCONUS) and Emergency Tracking Accountability System (ETAS) (CONUS). These systems use PCs, laptops and mobile handheld devices and computers that are networked via wireless, satellite,

LANs, and WANs communications to co-located laptop and/or central DMDC database servers. For additional NTS/ETAS Information reference Appendix F.1 thru F. 5.

3.4.4 The Joint Asset Movement Management System (JAMMS) is a technology application developed to capture movement and location information of federal government contractors, operating forces, and government civil servants, worldwide. These systems are standalone laptops that operate in both network connected and disconnected operations. For additional JAMMS Information reference Appendix T.1 thru T.2.

3.4.5 During the performance of this effort, DMDC anticipates the migration and consolidation of all computing workloads and their support functionality from their current data centers into a two-location private cloud environment which would provide platform-as-a-service capability for the organization and require a high degree of remote administration skillset.

4.0 REQUIREMENTS

The Contractor shall perform the following:

4.1 Worldwide Site Management Support

In this task, the contractor shall provide Installation Support Services which include timely on-site and telephonic site surveys, installations, de-installations, relocations, on-site training delivery, and technical/program management support that meet the quality levels identified in Appendix X, "Performance Requirements Summary". The task also requires that the contractor shall provide support of contingency operations for RAPIDS (deployments, mobilizations), DBIDS (physical access support), NTS/ETAS (evacuation support), and JAMMS (tracking consumption of authorized government services (AGS) and movement of deployed personnel).

Specifically:

4.1.1 The Contractor shall:

a. Perform and coordinate all site actions as noted above or associated with DMDC, the site point of contact (POCs) provided by the Government and other existing DMDC support contractors.
b. Maintain an up-to-date site action schedule within the Configuration Management Database (see Section 4.6).
c. Track all site actions planned to include: site surveys, installations, upgrades, relocations, and de-installations.

4.1.2 The Contractor shall:

a. Maintain a Quality Management System that complies with applicable Service specifications. For support of shipboard alterations refer to, NAVSEA Tech Spec 9090-310 G (see Appendix G) and NAVSEA Standard Item 009-04
b. Accomplish all Navy shipboard work as directed by and IAW NAVSEA standards and IAW NAVSEA Standard Items.

4.1.3 The Contractor shall:

a. Administer site certificate support for DMDC applications in accordance with Appendix D.6 –"DMDC Security Appendix". DMDC applications and data require a vast majority of data be encrypted during transmission. The contractor shall coordinate and obtain user or machine based certificates required for PKI authentication of communication endpoints.
b. Track expiration dates to identify certificates requiring replacement; obtain and deploy needed certificates in a timely manner to prevent any disruption of service to customer or DMDC sites. As part of task transition, an export of certificates from the current contractor should be made available through the DMDC Registration Authority Team.

4.1.4 Project/Program Management Support

4.1.4.1 The Contractor shall document technical solutions and associated cost quotes, by contract line item number (CLIN), in a Government-approved format. DMDC has multiple programs that are jointly funded by DMDC and the Services. All CLIN sheets shall be delivered within three (3) business days of the request unless an extension is approved by the Government. CLIN sheet preparation is generally to support new or upgraded equipment installations or for Service replacement of lost, stolen or user-damaged items.

4.1.4.2 The Contractor shall participate in calls, conferences, and meetings and shall prepare informational briefing materials to support the administration and execution of activities under the scope of this PWS.

4.1.4.3 The Contractor shall deliver:

4.1.4.3.1 **Monthly Progress Reports:** The Contractor shall submit monthly progress reports no later than the 20th workday of every month to the DMDC POC and the GSA COR. Requirement for resubmission based on inaccurate/insufficient detail will be at the determination of the Government. Any minor errors or inaccuracies shall be captured in the GSA IT Solutions Shop (ITSS) portal for the record and the report accepted as final. Monthly Progress Reports shall be uploaded to ITSS.

The Monthly Progress Report submitted shall summarize activities for the preceding period, milestones achieved/missed, and shall describe any problems encountered or anticipated. It shall include a maintenance trend analysis for the top six (6) component failures for the month by programs at the replacement unit level. It shall reflect the current fiscal status of the task order providing an accounting of the level of effort and funds expended and currently remaining, and any open hardware/software deliveries. The progress report shall provide the actual performance metrics including specifics to support the AQLs for all tasks of the task order.

4.1.4.3.2 **Technical Reports/Study:** When requested by the Government, the Contractor shall electronically provide a technical report/study in accordance with the

format specified by the Government to the Contracting Officer Representative (COR) and Technical Point of Contacts (TPOCs). A Technical Report/Study would be required, such as, when the contractor performs a market analysis for new hardware required for DMDC application functionality. The programs requiring studies and/or analysis change annually. The Government anticipates that approximately 6 technical reports/studies per contract year across all programs.

4.1.4.3.3 **Senior Management Review (SMR):** The Contractor shall meet with DMDC monthly, generally the last week of the month with the specific date specified by DMDC. The written deliverable shall be delivered three (3) business days in advance of the meeting. The Contractor shall provide an oral and written analysis in accordance with the format specified in Appendix M, "DMDC Senior Management Review Format".

4.1.4.3.4 **Meeting Agendas:** The Contractor shall electronically provide an agenda for each meeting two (2) days prior to the meeting. An example is the bi-weekly RAPIDS and DBIDS Program Management meetings. As needed the contractor shall prepare agendas and provide technical experts to lead/participate in periodic ad hoc meetings (e.g. team meetings to assess viability of a hardware solution; tiger teams to investigate failure issues, etc.).

4.1.4.3.5 **Meeting Minutes**: The Contractor shall electronically provide meeting minutes for each Bi-Weekly Program Management meeting and the Senior Management Review Meetings within three (3) days after the meeting or as needed following ad hoc meetings.

4.1.4.3.6 **Risk Mitigation Plan:** The Contractor shall implement a task order-wide Risk Mitigation plan and shall electronically provide the plan to the Government within the first thirty (30) business days of the task order award. The Contractor shall assess, evaluate, document, and manage risks associated with the performance of this Task order. The Contractor shall be responsible for creating, modifying, maintaining and implementing the plan.

4.1.4.3.7 **Contractor Discrepancy Resolution (CDR) Report:** In the event of unsatisfactory contractor performance, the CO will issue a CDR that will explain the circumstances and findings concerning the incomplete or unsatisfactory service. The contractor shall acknowledge receipt of the CDR and respond in writing within five (5) business days as to how he/she shall correct the unacceptable performance and avoid a recurrence. The Government will receive the contractor's corrective action response to determine acceptability and will use any completed CDR as part of an overall evaluation of Contractor performance when determining present or future contractual actions.

4.1.4.3.8 **Annual Update to the Technical Roadmap**. The contractor shall provide this report 60 days after award of each option period. The update shall include schedule and milestones for all technology and a recommended approach to optimizing the Total Cost of Ownership.

4.1.5 Provide New Site Support

4.1.5.1 The Contactor shall perform site surveys either telephonically or on-site in accordance with schedules developed in concert with DMDC no later than 30 days prior to each scheduled installation or relocation, unless otherwise directed by the Government. All DBIDS site surveys are conducted at the physical location. Site survey formats will be mutually agreed upon between the contractor and DMDC upon award.

The Contractor shall submit a site survey report no later than two (2) weeks after completion in accordance with the format specified by the Government.

4.1.5.2 The Contractor shall:

a. Install all DMDC-provided GFE and COTS hardware and software purchased for scheduled site installations.
b. Provide all the tools and support necessary to complete installations and ensure the site is operational.
c. Provide training to site personnel on the equipment/application installed as noted in Section 4.1.7 below, when requested.

4.1.5.3 The Contractor shall provide all services to conduct an on-site site survey independent of an installation for RAPIDS and DBIDS. Site survey formats will be mutually agreed upon between the contractor and DMDC upon award.

4.1.6 Modification/Upgrade/Troubleshooting of Existing Site

4.1.6.1 The Contractor shall support hardware and software modifications, upgrades and periodic troubleshooting. These may be performed on site or require telephonic coordination with the end user. The Contractor shall provide the support necessary to complete the upgrades and ensure the site is operational in order to meet the requirement of Appendix X, “Performance Requirements Summary”.

4.1.6.2 The Contractor shall support equipment relocations including site coordination, de-installation, packing, shipping, and reinstallation of all components of the system as each particular relocation dictates. Relocations include moving equipment at a site or base within the current room, between different rooms, and between different buildings. The Contractor shall provide the support necessary to complete relocations and ensure the end site is operational. If practical and approved by the Government, some sites will perform their own self-help relocations with telephonic assistance from the Contractor, as needed.

4.1.6.3 The Contractor shall provide all services required to support equipment de-installations including site coordination, de-installation, packing, and shipping equipment to the appropriate destination (contractor's GFE inventory, or another location, as determined by the Government). For example, when a de-installation does not require on-site contractor support, coordinate the return of the de-installed hardware with the site,

provide proper packaging materials to the site if all equipment is not being excessed, and provide any assistance required by the site to complete the self-help de-installation. Hardware that has not been received at the destination within 10 days of coordinated site closure should be reported to the Government for further coordination.

4.1.6.4 Whenever site actions require that equipment be excessed to a site, the Contractor shall provide the site point of contact (SPOC) with a pre-filled Requisition and Invoice/Shipping Document (Department of Defense [DD] Form 1149 (See Appendix H.1) for signature, documenting the serial numbers of the equipment being excessed to the site. The government will provide or approve the application required to sanitize media. The Contractor is required to support the excess of Government property. The Contractor shall request that the DD Form 1149 be signed by the site POC and returned to the Contractor, for updating the Configuration Management Database that is maintained by the Contractor (see Section 4.6.1.3). The Contractor shall notify the Government's designated DMDC POC of sites that do not comply with returning the signed DD Form 1149 to the Contractor within two (2) weeks. Whenever a computer (server, workstation, laptop/notebook, or handheld computer) is being excessed, ensure that a DoD-approved disk wipe/memory wipe has been performed before excessing it to the site or the Contractor shall arrange for the computer to be returned to the Contractor's facility to be wiped IAW DoD 5220.22-M requirements and National Industrial Security Program Operating Manual (NISPOM) standards. For excessed equipment from the Contractor's location, the Contractor shall prepare the DD Form 1348-1a (Appendix H.2) for DMDC review and coordinate with Defense and Reutilization and Marketing Office (DRMO) for pick up.

4.1.7 Worldwide Training Support & Delivery

4.1.7.1. The Contractor shall provide on-site training at newly installed sites, or other specified locations, such as conference or service training centers to support DMDC applications. Follow-up user training is usually via DMDC's web-based Learning Management System (LMS) although in some instances (i.e., complete site user personnel turnover) training on-site will be required. Generally, the Contractor shall provide full hands-on training for new installations or significant application changes/upgrades. Training shall include instruction on hardware (i.e., proper printer cleaning, deployable assembly, etc.) and application usage. The Contractor Instructors shall maintain current on policy at all times.

4.1.7.1.1 DMDC has a separate training courseware development contractors who are responsible for developing all application training materials. The separate training courseware development contractors may require review and input on an ad hoc basis from the contractor. Training coursework will be provided to the contractor for delivery. Currently, DMDC uses Joint Knowledge Online to deliver online training.

4.1.7.2 The Contractor shall provide telephonic training and/or installation support. In some instances, support will be required at a remote deployed site. The Contractor shall conduct full training to walk the user through the proper set up and use of hardware

and software. The Contractor may be required to deliver training materials to these locations.

4.1.7.3 The Contractor shall submit a Training Checklist in the approved Government format for all on-site training within fourteen (14) calendar days of the visit (see Appendices D.8, D 8.1, E.8 and F.5 for an example of the existing "DMDC Training Checklists").

4.1.8 Contingency Support

4.1.8.1 The contractor shall ensure readiness and availability to support all contingency operations and Service operational readiness, the Contractor will be provided the Government furnished equipment (GFE) listed below for maintenance/storage and the Contractor shall support shipment of the following systems within 24 hours:

a. 40 - 50 desktop or deployable RAPIDS workstations,
b. 10 NTS conveyance and 25 NTS registration workstations,
c. 10 DBIDS registration workstations,
d. 20 DBIDS gate workstations (inclusive of required handheld scanners),
e. 15 DBIDS mobile gate kits and a minimal number of added peripherals specifically required to support short lead-time DBIDS installations in our forward deployed areas such as 10 each indoor and outdoor hand geometry units, 10 iris scanners, and 10 10-print capture devices.
f. 25 JAMMS mobile kits

As part of task order transition, custody of existing contingency systems will be transferred from the incumbent to the incoming Contractor. Throughout the task order period, the Contractor shall sustain the required base of equipment and provide requests for GFE equipment to replenish stock readiness. The Contractor shall notify the Government if, at any time, the stored hardware or software is no longer compatible with the current production system baseline. The required base of equipment for contingency support may evolve over time as production system baselines change. DMDC will not provide space at Government locations for storage of government furnished contingency systems. The Contractor shall provide storage for equipment identified above.

4.1.8.2 The contactor shall send the required personnel to provide user instruction on systems setup/use. For RAPIDS this includes performing Local Registry Authority (LRA) functions using a deployable workstation to issue CACs. For NTS/ETAS, DBIDS, and JAMMS, this may include providing on-site training and hands-on operational support. The contactor shall send the required personnel to provide user instruction on systems setup/use. On some occasions when emergency requirements arise, DMDC has the need to send personnel with the systems to provide user instruction on system set up/use and as directed and authorized by the Government, the contractor shall act as the operator for the applications.

In such situations, as noted in Section 4.1.8.1, the equipment shall be shipped within 24 hours of notification. As required, the Contractor shall provide the on-site support with the equipment within the 24 hours of notification.

4.1.9 Operations Planning, Logistics, and Implementation Support

4.1.9.1 Provide support for operations planning and implementation activities for DMDC programs. Currently, the largest programs are RAPIDS and DBIDS.

4.1.9.2 Process site-related requests submitted by DMDC project managers and Service Project Officers within the specified timeframes below. There will be times when requests must be processed immediately.

4.1.9.3 Log each request as an action item (AI) in the Automated Information Tracking System (AITS) (See Appendix AB, AITS User Guide) database (SharePoint), assign the necessary tasks to the appropriate groups and manage each request to completion. AIs should be generated as quickly as possible upon receipt of the request but no later than two (2) days from receipt unless additional information is required. Requests include but are not limited to: installation of new sites, increases/reductions/transfers of equipment, relocations (both self-help and installer-assisted), communication connectivity changes, site closures, support for hardware and/or software upgrades, and support for special events (e.g., Retiree Days).

4.1.9.4 In conjunction with the AIs, coordinate the activities of multiple DMDC teams and contractors to provide hardware, software, communications, and/or training, as dictated by the type of schedule and location; e.g., CONUS, hardware lifecycle upgrade, software upgrade, etc. at the direction of the Government.

4.1.9.5 Develop, maintain and/or monitor installation and fielding schedules. Schedules are also entered into AITS and sent to the appropriate groups for execution.

4.1.9.6 Provide information about site actions and schedules to all relevant parties to include other DMDC organizations and personnel, Service leads and site personnel.

4.1.9.7 Design, develop and/or maintain DMDC databases and documents used to manage Customer Operations tasks. These tools, including AITS, the Engineering Change Proposal (ECP) tool, and the Travel Request Tool, are currently hosted in SharePoint. Upgrade to new technology as required.

4.1.9.8 Review and validate shipping invoices for accuracy prior to approval for payment by the Government. In the case of erroneous charges, coordinate with the shipper to adjust the charges and invoice the sender. Reviews shall be complete within one week from date of receipt.

4.1.9.9 Generate identified reports on an ongoing basis (frequency varies by report). Reports include, but are not limited to, the monthly CAC Failure Report, the monthly

RAPIDS user roster/non-compliance report (SSM/VO Report), and the RAPIDS Quarterly Workstation Utilization Report. Reports are due within five (5) business days of receipt of the necessary data. In addition, generate the Annual RAPIDS Workstation Allocation Review spreadsheet based on the most recent quarterly utilization report. The report is due to the Government for review six (6) weeks prior to the date of the review with the Service Project Officers. Produce ad hoc reports and queries as requested by DMDC.

4.1.9.10 Assist with the development of operational and functional documentation to support program user instructional material such as Standard Operating Procedures (SOP), the Messages of the Day (MOTD), and Helpdesk knowledge articles. With the exception of action items, post all documents to the government designated locations.

4.1.9.11 Develop and maintain operational documentation (SOPs) for internal Customer Support tasks and processes. SOPs shall provide clear, complete directions that can be easily followed by someone new to the task. All SOPs are stored in the Customer Operations section of the shared electronic library

4.2 Worldwide Networks and Communications Engineering Support

This task requires the contractor to provide quality and timely network and infrastructure architecture design, proactive communications performance analysis and Service/Agency coordination which includes DMDC tenant applications and coordination security posture. These tasks require customer interaction, optimized system performance, and enhanced network security.

4.2.1 The Contractor shall provide network operations support for architecture and design of communications connectivity for required DMDC application execution, installation/relocation of hardware, and crucial network changes. Networking services shall be provided through a single point of contact for network architecture design (in cooperation with local and regional Uniformed Service communications support organizations). Coordinate circuit moves, add-ons, configuration changes, perform routine maintenance related tasks, and maintain router security based on industry best practices and in accordance with DoDI 8500.01 Cybersecurity, 8510.01 Risk Management Framework (RMF), and the National Institute of Standards and Technology (NIST) 800 series publications. Once the site is fully operational, the DMDC Customer Contact Helpdesk will troubleshoot and work any issues. Support requires significant coordination and communication with other government and commercial activities as well as coordination with various individuals within DMDC.

4.2.1.1 The Contractor shall support the daily operations for the Cisco ASA and switches for required product architecture.

4.2.2 The Contractor shall interact with sites and regional organizations to maintain current architecture and work closely with DMDC to design, develop, and implement new technologies and configurations as application communications requirements evolve.

DMDC applications rely on the base/facility where the workstation/server is located, to provide the communications for the application. Each site has a communications support/control organization and several of the Uniformed Services have regional or Service-wide communications support/control organizations. DMDC interacts at the Service level, and assists at the base and regional levels.

4.2.2.1 The Contractor shall provide daily support for network firewalls installed at DoD installations in support of fielded applications. This includes support for the 1 primary and 1 fail-over DBIDS firewall located within the DMDC enterprise, as well as 1 DMDC controlled firewall per site (currently Cisco ASAs).

4.2.3 The Contractor shall provide wireless network operations support for architecture, design and engineering of secure wireless network solutions required for DMDC applications, to include system integration, deployment, configuration and administration. The Contractor shall coordinate wireless network updates and changes for application execution, installation/relocation of hardware, and network changes with site communications support/control organizations and Uniformed Services regional or Service-wide communications support/control organizations. The Contractor shall coordinate with site communications support/control organizations and Uniformed Services regional or Service-wide communications support/control organizations to authorize wireless network devices required for DMDC applications in Wireless Intrusion Detection Systems (WIDS) implementations. The Contractor shall perform routine maintenance related tasks and maintain wireless network security based on industry best practices and in accordance with DoDI 8500.01 Cybersecurity.

4.2.4 The Contractor shall coordinate with site and service security agencies in conjunction with DMDC to maintain mutually acceptable security risk posture, forward any requests for Cybersecurity accreditation documentation to DMDC, and provide support for assessment and authorization (A&A) and Federal Information Security Management Act (FISMA) security control testing and remediation efforts.

Local and Service-level IA organizations require documentation, testing and certification of DMDC programs for deployment on their networks. The Contractor shall assist the site and DMDC in supporting the A&A and FISMA efforts as technical SMEs and system administrators. The Contractor shall assist the responsible Government POCs with the preparation of the Supporting Certification Documents, the testing environment, and POA&M efforts for A&A and FISMA testing conducted at DMDC facilities, including OCONUS support centers.

4.2.5 Communications Performance Analysis

4.2.5.1 At a minimum, the Contractor shall conduct baseline performance analyses on a quarterly basis and supplement such quarterly baselines with additional analyses when required. The Contractor shall provide communication performance analysis and documentation due to complaints of sustained poor system performance or to test compatibility with a Service unique architecture. The Contractor shall work in

coordination with Site personnel and site or Service level network administrators to simulate operations and obtain and analyze network data captures at the remote site. As necessary, the Contractor shall coordinate with DMDC network administrators to obtain and analyze data captures of the traffic on the DMDC network and shall document results.

4.2.5.2 The Contractor shall perform and document network traffic performance analysis using network traffic shaping hardware to determine system performance using simulated low-bandwidth/high latency (or other simulated parameters) network conditions.

4.2.6 Client Management Support

Cybersecurity is directed by the DMDC Cyber Security Division. Security compliance and patch management is a crucial element in systems administration. IT security planning, implementation, and compliance is an integral part to all work performed at DMDC and, therefore, participation is a shared responsibility. The Contractor shall be responsible for continuing to maintain security compliance support. Security compliance support shall encompass researching, testing, and deploying patches for remediation of vulnerabilities identified by security tools managed by the Cyber Security Division. Most of the tasks listed in this section can be supported remotely. However, there are frequent times when it is necessary to work with the RAPIDS workstations located in the beta test lab in the Mark Center. This occurs predominantly during active hardware and software tests and to research issues reported from the RAPIDS users.

4.2.6.1 Provide information assurance support personnel to consult on DMDC system compliance with the DoD Risk Management Framework (RMF) requirements. The position requires the person be knowledgeable of RMF and NIST requirements (ATO/IATO/Scorecards) in order to review and validate documents presented by current and potential DMDC customers. This task does NOT include the actual RMF testing. It includes response and remediation of RMF testing and requirements only. On occasions, there might be ongoing consultation required outside of the formal yearly RMF testing, e.g. when a new Information Assurance Vulnerability Alert (IAVA) is released or when a system vulnerability is found.

4.2.6.2. Enterprise Mission Assurance Support Service (eMASS) is the current tool used for the RMF Assessment and Authorization (A&A) at DMDC. Populate eMASS with the necessary information to validate cybersecurity controls are met. This includes System Security Plan, Plan of Action & Milestone (POA&M), Implementation Plan and Risk Assessment. Create or update system and program artifacts in eMASS to demonstrate compliance of NIST SP 800-53 controls [e.g. Security Standard Operating Procedures (SSOP), architecture diagrams]

4.2.6.3 Provide support to the Cybersecurity Division for Risk Management Framework (RMF) audit activities. On behalf of the program, respond and report on information and data call requests pertaining to the A&A audit. The function and the POC for the program by facilitating and coordinating with the Cybersecurity Division when requested. Provide weekly status report at a minimum or as directed by DMDC.

4.2.6.4 Assured Compliance Assessment Solution (ACAS) is the DMDC vulnerability scanning tool owned and operated by the Cybersecurity Division. Request and submit ACAS view-only account access for system vulnerabilities. Remediate and apply applicable patches or fixes (configuration changes) on identified security vulnerabilities on DMDC systems as reported in within ACAS, eMASS, STIG or HBSS. Provide a Plan of Actions and Milestones (POAM) and STIG Deviation/Non-Compliance report for remediation actions that cannot be accomplished by the Cybersecurity Division assigned completion date. Vulnerabilities are completed for critical findings within 7 days of discovery and high within 21 days of discovery. STIG configuration items are to be correctly upon identification by the Cybersecurity Branch. Remediation requires installation, configure, upgrade, test and troubleshoot computer software to maintain security policies. Remediation also includes but not limited to utilizing Windows Remote Desktop Connection to remotely connect and patch security vulnerabilities on non-compliant systems.

4.2.6.5 Ensure security compliance and provide compliance reports.

a. Validate systems compliance by using the available compliance verification tools operated by Cybersecurity such as ACAS, HBSS, etc. This position requires access to these verification tools and will need the appropriate background investigation and security clearance.
b. Provide weekly compliance reports to Customer Operations using the available reporting tool such as ACAS, HBSS, CA IT Client Manager (ITCM), etc. ACAS and HBSS are the authoritative sources for verifying compliance but DMDC tools such as the CA IT Client Manager (ITCM) may be used if necessary.
c. Apply vendor supported security patches on a continuous and timely basis per DoD and DMDC policy. Support third-party software updates and apply definitions to all applicable DMDC systems.
d. All new IT assets built under this contract and baseline images must go through the DMDC Pre-production process and approved by the Cybersecurity Division prior to operation in a production environment. Perform Information Assurance Vulnerability Management (IAVM) compliance patching on applicable assets on DMDC networks. Install, configure, and test patches and changes required by IAVM issuances.
e. All COTS software or hardware patches, updates, firmware must come from the DoD patch repository. Exceptions must be approved by the Cybersecurity Division prior to engagement.
f. Review the security compliance scanning tool reporting metrics for the RAPIDS clients and produce a monthly report indicating non-compliance, anomalies, and workstations that have not been scanned in the last 30, 60, 90 or more days. The current tool is the Assured Compliance Assessment Solution (ACAS).
    1. Recommend on a weekly basis of workstations that have not connected for thirty (30) days or more and can be disabled for cyber non-compliance.

2. Ensure patches are created and deployed for vulnerabilities reported on ACAS.

4.2.6.6 Update the internal Plan of Action & Milestones (PoA&M) tracking worksheet on a weekly basis to add new vulnerabilities and submit a PoA&M for those vulnerabilities, ensure milestones are met on existing PoA&Ms and delete superseded PoA&Ms. DMDC estimates that this will require submitting up to 10 new PoA&Ms per month, resubmitting up to 2 PoA&Ms per month and supporting special events (e.g. audit) up to twice per year which would require submitting an additional 5 PO&AMs in those months.

4.2.6.7 Host Based Security System (HBSS) is owned and operated by the Cybersecurity Division. Support the Cybersecurity Division in troubleshooting point product deployment and operational issues. Troubleshoot client/agent ePO non-connectivity issues. Provide proposals for HBSS firewall rules, IDS and anti-virus and application whitelisting. Provide HBSS weekly compliance report.

4.2.6.8 Submit new HBSS point products upgrades to QA for testing.. Complete QA notification form and coordinate with QA and Cyber Ops. Upon QA completion, coordinate beta testing with BRTT team.

4.2.6.9 Facilitate a weekly RAPIDS security meeting and report on IA status (e.g. ACAS, HBSS, CCRI, IAVA, STIGS, POAMs, TASKORDs, etc.). Provide meeting minutes within three (3) business days of the meeting. Coordinate with Cybersecurity Division for compliance reporting.

4.2.6.10 Act as a liaison between DMDC and C/S/A telecommunications organizations for both new installations and ongoing operations. Assist with installation and planning, evaluation of firewalls/security access, network latency, ports and protocols, and provide problem escalation resolution related to site infrastructures and wide area networks. Recommend solutions consistent with DMDC standard implementations.

4.2.6.11 As a liaison between DMDC and the customers' network/firewall POCs, support activities related to testing and implementation of cybersecurity products. Additionally, research problems associated with the cybersecurity products (e.g., HIPS blocking of new profiles, dropping of connection during encoding, etc.). Support requests from sites for security scans (i.e., submit the requests to systems, facilitate timing of the scans, review results, direct any needed remediation efforts and deliver the results to the requestors). Monitor site compliance to security requirements (i.e., regularly connecting to the VPN, downloading security patches, etc.)

4.2.6.12 Provide support to the fielded workstations. Assist in resolving network-related problems at sites that remain unresolved pass SLA standards. Support new installations. As needed, update documents related to telecommunications and security (e.g., the RAPIDS Standard Security Operating Procedures (SSOP).

4.2.6.13 Support quarterly updates for the RAPIDS afloat workstations. Obtain an image with all new updates (latest version of RAPIDS, drivers, security patches, etc.), along with installation instructions. Create the CD (instructions included) and send it to SPAWAR for testing of the installation process. Review any requests for modifications to the instructions and, if in agreement, make the changes. Once SPAWAR approves, burn enough CDs for all the ships and arrange for mailing/shipping of the CDs, to include verifying addresses to the extent possible.

4.2.6.14 Monitor program telecommunications for compliance with all applicable DoD telecommunications policies and procedures.

4.2.6.15 Support and coordinate network scans required for software and hardware upgrades, maintenance replacements, relocations, deployments, redeployments, etc.

4.2.6.16 As needed, provide ACAS scan report for new installations, life-cycle and maintenance replacements for the Navy on NMCI/NGEN network. The ACAS scan report must show that the vulnerabilities have been remediated or a PoA&M is submitted for vulnerabilities that cannot be remediated.

4.2.6.17 Coordinate with the appropriate teams (i.e. Cybersecurity Division, IT Ops, RIT, SDO, etc.) on vulnerabilities identified during a security scan (e.g. ACAS Compliance or Vulnerability scans, TASKORDS, CCRIs, Audits, etc.)

4.2.6.18 Provide ACAS scan report in support on a Command Cyber Readiness Inspection (CCRI) for the local RAPIDS site. Handle on average 20 assets per month. Responsible for troubleshooting, mitigating and patching workstations that are not compliant.

4.2.6.19 Perform preliminary technical reviews and assessments of baseline documentation, System Requirements, Change Requests, Concept of Operations, Vulnerability Analyses, and Migration Plans.

4.3 Outside the Continental United States (OCONUS) Support

This task requires Technical and program management support which entails direct interaction with operational sites and Service points of contact, inventory and shipment management, testing and distribution of software, database administration, and system management support in identified Theaters (PACOM, EUCOM, CENTCOM, SOUTHCOM, AFRICOM).

4.3.1 Project and Program Management Support

4.3.1.1 The Contractor shall provide project and program management support for OCONUS installations. As an example, occasionally OCONUS support centers will be contacted by customers/beneficiaries requesting liaison assistance regarding a multitude of DMDC technical services/products. These calls are considered program support, not helpdesk.

This work includes coordinating directly with end users on questions or concerns about how DMDC applications function, questions on data issues associated with benefits or privileges of DoD or DoD-affiliated personnel and for informational support on DMDC products.

4.3.1.2 The Contractor shall develop and implement schedule to support new software releases to ensure seamless deployment to the end-user workstations. RAPIDS will use Software Delivery Option (SDO) and DMDC approved software management tools (i.e. SCCM and WSUS).

4.3.1.3 The Contractor shall provide direct hardware and software support to customer sites for troubleshooting application software and hardware. For site information, refer to Appendix D for RAPIDS, Appendix E for DBIDS, Appendix F for NTS/ETS, and Appendix G for JAMMS. Primarily this support is for the DBIDS, NTS, and JAMMS applications because the DMDC Customer Contact Center Helpdesk does not have direct access to OCONUS systems.

4.3.2 Customer Support

4.3.2.1 The Contractor shall interface with the Joint Uniformed Services Personnel Advisory Committee members and Defense Human Resources Activity (DHRA) policy representatives to coordinate OCONUS policy inquiries.

4.3.2.2 The Contractor shall provide liaison activity support to regional Service representatives and conference support by coordinating with the Service/Agencies impacted and develop any/all required documentation to respond to customers, conducting analysis, gathering requirements, and developing documents.

4.3.2.2.1 Liaison activities include providing support in theater for DMDC applications by coordinating directly with end users for questions or concerns about how the applications identified under the scope of this task order work, questions on data issues associated with benefits or privileges of DoD or DoD-affiliated personnel, and for informational support on DMDC products (i.e., “What form do I need to fill out to add a user at Site 123?” or “My General wants to know when the SSN will be removed from the barcodes on the card?” or “We need to get a card to a person in North Nowhere, how can I do that?” In support of investigations, examples include questions such as: “Who was driving the white Impala that came through the gate at 1900?” or “What is this person's access history at Camp Somewhere?”)

4.3.2.2.2 Conducting analysis may include researching the answers to all inquiries received, coordinating with the associated DMDC application POCs, coordinating with the Service/Agency impacted and develop any/all requirements documentation to respond to customers. Documentation may include drafting white papers assessing the issue and recommendations, drafting correspondence for Government release, developing

milestone schedules or user tip sheets, etc. Such documentation shall be maintained and updated as required.

4.3.3 Database Management and Support

4.3.3.1 The Contractor shall provide services associated with the functional area of Database Management and support. Server Infrastructure information is provided in Appendix I, "Server Infrastructure". The Contractor shall provide Database Administrator (DBA) services and shall assist DMDC in modifying both the tools and the underlying database to maintain operational effectiveness. The scope of this work includes:

- Database administration
- Database performance tuning, backups, and monitoring.
- Enhance the existing database processes and applications
- Data Modeling
- File processing (submission processing, quality control, and required backups)
- Data warehouse (maintain, insert data)
- Support of end-to-end processing such as data and acquisition analyst type activities including PL/SQL and SQL loader coding, web report generation applications, and exception handling to ensure the safe migration of data into and reporting from the Data Warehouse
- Data quality
- Assist in the areas of Data Quality Control and Quality Assurance in verifying the accuracy and completeness of the data found in the database
- Identify and correct errors in the existing trouble shooting documentation (e.g. Frequently Asked Questions (FAQs), knowledge base articles, etc.) related to database issues
- Support the ongoing database implementation, enhancements, changes required by law or directed by DMDC
- Support retrieval of data from the database and report generation for analysis and ad hoc requests
- Define requirements for hardware and software to implement integrated databases
- Data engineering, mapping, standardization, migration, transformation, security and warehousing services
- Evaluate, and potentially use, database management tools adopted and approved by DMDC Architecture Review Board (ARB)
- Develop data maintenance applications and reports
- Database patching
- Migration of the database from one version of DMDC software to another
- Merging of several like databases for DBIDS products into one database
- Monitor performance of the databases
- Manage space, monitor resources, refine and improve database performance
- Participate in periodic Disaster Recovery Action planning and testing of production databases, including:

- Developing/reviewing data recovery procedures for all media.
- Planning for and accomplishing actions needed for continued database availability in the event of contingencies, natural disasters or other unplanned events.
- Testing data recovery procedures for all media on a periodic basis.
- Adhering to the DMDC Incident Response Policy (IRP). Documenting and responding to any disruption to the DMDC applications environments, including any unauthorized intrusion that compromises operations.

- Support local command RFM processes.
- Adhere to the DMDC Incident Response Policy (IRP). Document and respond to any disruption to the DMDC applications environments, including any unauthorized intrusion that compromises operations.

Oracle Enterprise Manager will be provided as GFE post award to the contractor to accomplish the requirements of this task.

4.3.4 System Management and Support

4.3.4.1 The Contractor shall provide services associated with the functional area of System Management and Support. The Contractor shall provide System Administrator (SA) services to DBIDS sites. Server Infrastructure information is provided in Appendix I. The Contractor shall assist DMDC in modifying both the tools and the underlying server infrastructure to maintain operational effectiveness. The scope of this work includes:

- Provide Active Directory installation and administration
- Support installation and administration of the following systems:
  - Remote Desktop Software (e.g. Dameware, RDP)
  - System Deployment and Management Solutions (e.g. WSUS, SCCM)
  - Antivirus Management Packages (e.g. McAfee, Symantec)
  - DoD Enterprise Information Assurance (IA) Tools (e.g. HBSS, Retina)
- Ensure compliance with Cyber Security regulations governing security patching and vulnerability scanning using DoD approved tools and utilities
- Perform backups.
- Enhance the existing system processes and applications
- Identify and correct errors in the existing trouble shooting documentation (e.g. FAQs, knowledge base articles, etc.) related to server issues
- Support the ongoing server implementation, enhancements, changes required by law
- Generation of server status and utilization reports
- Define requirements for hardware and software to implement server infrastructure
- Maintain, monitor and report on the overall health of the server and workstations.
  - Onsite infrastructure (including gates) availability shall exceed 99.9% uptime outside of scheduled maintenance periods.

  - Obtain approval for scheduled outages. Once approved, notify customers of scheduled outages, expected length of the outage, and restoration of services.
  - In the event of an unscheduled outage, begin diagnosing the affected systems and provide DMDC customers outage notifications within 2 hours.
- Evaluation, and potentially use, system management tools adopted and approved by DMDC Architecture Review Board (ARB)
- System patching
- Migration of systems from one version of DMDC software to another
- Merging of several like infrastructures for DBIDS products into one common infrastructure
- Monitor performance of the server infrastructure
- Manage space, monitor resources, refine and improve server performance
- Participate in periodic Disaster Recovery Action planning and testing of production servers, including:
  - Developing/reviewing server recovery procedures.
  - Planning for and accomplishing actions needed for continued server services availability in the event of contingencies, natural disasters or other unplanned events.
  - Testing data recovery procedures for all media on a periodic basis.
  - Adhering to the DMDC Incident Response Policy (IRP). Documenting and responding to any disruption to the DMDC applications environments, including any unauthorized intrusion that compromises operations.
- Adhere to the DMDC Incident Response Policy (IRP). Document and respond to any disruption to the DMDC applications environments, including any unauthorized intrusion that compromises operations.
- Support local command RFM processes.

4.3.5 Inventory Management

4.3.5.1 The Contractor shall manage receiving and storing of DMDC (e.g., RAPIDS, DBIDS, NTS/ETAS, and JAMMS) inventory to include maintaining inventory, tracking and delivery of systems at each of the DMDC Support Centers (DSCs) in Korea, SWA and Europe and ensuring all systems are up to date and ready to field at all times for emergent requirements.

4.3.5.1.1 The Contractor shall retrieve failed equipment from DBIDS sites and work directly with manufacturers and DBIDS sites to facilitate repairs/replacements.

4.3.5.1.2 The Contractor shall provide personnel capable of communicating effectively in the language of the locality where they are working. (Note: although at most bases supported OCONUS, English language speakers are sufficient; in certain locations – most specifically, – knowledge of the local language is highly valuable).

4.3.6 Shipment Management

4.3.6 OCONUS facilities in Europe and Korea keep a limited supply of cardstock media and consumables for identified systems (i.e. cards, electromagnetic sleeves and printer consumables, ribbons, transparency film, cleaning kits) on hand to support emergency shipments that cannot be sent from the CONUS DSC in time to support operational requirements in the field. The Contactor shall comply with all local Customs requirements for shipment of cardstock and consumables using Government-provided shipping accounts. Some of the items may be required to ship through Army Post Office/Fleet Post Office (APO/FPO) channels. The Contractor shall coordinate shipment with the site users and update tracking in the Integrated Logistics Portal web tool for all emergency shipments.

It should be noted that cardstock and consumables are tracked in the DMDC Inventory Logistics System (ILP). The Contractor will be granted access to the ILP. All cardstock and consumables are procured by DMDC and will be provided to the Contractor to manage.

4.3.7 Testing Support

4.3.7.1 The Contractor shall perform hardware and software beta testing to validate and ensure whether components tested and approved in the laboratory test environment will operate effectively in the production environment. This consists of rigorous quality assurance, user acceptance and external beta testing. The Contractor shall inform each site identified by DMDC as a Beta test site of the testing scope and timing and the Contractor shall communicate any schedule and/or scope changes with applicable stakeholders. The Contractor shall install hardware and/or software, train users, observe and monitor systems functionality for the duration of the beta test, and report any findings/problems identified to DMDC. The Contractor shall provide the written test plans and the documented test results.

4.3.7.2 The Contractor shall perform unit acceptance testing of new software versions and components prior to user acceptance testing. The Contractor shall establish the environment for and coordinate user acceptance testing prior the deployment in a production environment. This testing is primarily for DBIDS and has historically occurred twice a year.

The Contractor shall perform beta testing to assess the application in accordance with the Government's User Acceptance Test Plan and support/assist users with questions during beta testing and liaison activities.

The Contractor shall provide documented user acceptance test results.

4.4 COTS Hardware and Software Support

In this task, the Contractor is required to purchase hardware and software products and services that are listed on the DMDC "Approved" hardware and software lists. The approved hardware and software lists can change over time and will require acceptance testing and engineering change proposals. These tasks also require the contractor to provide worldwide hardware and software technology solutions requiring different electrical standards, system integration, shipping support, and quality control. The contractor shall provide a solution that includes:

- TAA compliant equipment,
- Shipping and Handling from OEM to warehouse, and warehouse to site,
- Storage, and
- Loading software suite, security scans

4.4.1 The DMDC maintains a large infrastructure and also supports a number of projects leveraging that infrastructure that require purchases of hardware and system software for all DMDC databases, systems and applications. The hardware, software and the associated services are defined as optional as will be procured utilizing the following procedures:

The optional hardware and software products and services will be obtained on an as-needed basis through the exercise of options via option letters. Option letters will be numbered and incorporated into the Task Order via bilateral modification. Option Letters for priced hardware and software products and services will be issued bilaterally in ITSS, where the contractor will need to sign the modification prior to the Contracting Officer's signature. The contractor shall sign the modification or provide feedback to the Government within 48 hours of the Government's request for a modification signature.

Option Letters for approved Hardware and Software products and services:

To meet the hardware and software needs of DMDC and DMDC's clients, the DMDC COR will request CLIN sheets for each specific HW/SW purchase. These CLIN sheets shall act as the contractor's quote for the required HW/SW and the CLIN sheet pricing shall be valid for at least 60 days. At a minimum, each CLIN sheet shall include:

a. Action Item Number/Quote Number
b. Name of the Purchase
c. Unique Line Item number for each line item identified
d. Item Description for each line item identified
e. Quantity for each line item identified
f. Unit Price for each line item identified
g. Extended Total (Unit Price X Quantity) for each line item identified
h. Estimated Delivery Date for each line item identified
i. Total Cost of the CLIN sheet

The requested CLIN sheets do not bind the Government and can be obtained for research purposes only. The Government will accept the required CLIN sheets through Option

Letters issued by a GSA Contracting Officer via Task Order modifications in ITSS. The Contractor is not authorized to proceed with the purchase of HW/SW unless a modification is used by a GSA Contracting Officer.

One Option Letter may accept several CLIN sheets. Each CLIN sheet will have a standalone Task Item in ITSS. During invoicing, the contractor shall submit costs associated with the CLIN sheets to the ITSS Task Item associated with the respective CLIN sheet.

In the event that optional products and services require a work statement, the 'Request For Quote (RFQ) will include, at a minimum, the following information:

(a) Date
(b) End User
(c) Statement of Objectives (SOO), Statement of Work (SOW) or Performance Work Statement (PWS)
(d) Instructions for quote submission
(e) Quotation Due Date

The Contractor shall use the labor categories and product prices within the task order as the basis for the quote. If unique labor categories and/or ancillary products in the quote are required, the Contractor shall include the justification for their use and the basis for the pricing.

Option Letters for products and services that require the RFQ process may be issued unilaterally.

4.4.1.1 COTS HW and SW Management

The Contractor shall:

a. Provide CLIN sheets within three (3) business days of the request.
b. Provide Site Action Schedule Management.
c. Provide a work flow process that will provide the overall site action schedule and the current status on all planned actions.
d. Provide a quarterly report on software licenses and hardware maintenance renewals due in the next 120 days.
e. Provide status of delivery of hardware and software orders.
f. Provide project management on implementation services to ensure project is completed on time and within budget.

4.4.2 The Contractor shall furnish requisite COTS hardware and software materials and ship within required timeframes to support DMDC projects during peacetime and during times of mobilization and/or contingency operations. The scope of this work includes providing hardware, software, and shipping to support tasks worldwide. Requirements will be rated in accordance with the Defense Property Accountability System (DPAS) in a manner that meets mission needs.

4.4.3 The DMDC application environment is worldwide and requires hardware items to be available in versions that can operate from 110 volt (V), 60 Hertz (Hz) power with US

110V outlets and 220 V, 50 Hz power with 220V outlets as appropriate to country of operation.

4.4.4 The Contractor shall provide separate 110V and 220V CLINs as indicated in Appendix K, "Technical Specifications for COTS Hardware and Software". Sites that require equipment with non-standard power plugs will be specified by the Government.

4.4.5 The Contractor shall ensure that necessary hardware, software, and documentation are available to satisfy the technical specifications, provided at Appendix K, "Technical Specifications for COTS for Hardware and Software". DMDC will maintain and revise these specifications as hardware components and technology change as well as when the requirements of these DMDC systems change. All changes to the specific hardware and software purchased will be required to be certified by acceptance (see PWS Sections 7.3 and 7.4). As required, delivery shall be staggered to accommodate implementation schedules and/or site readiness.

4.4.6 The Contractor shall maintain COTS hardware and software purchased under this task order. Equipment proposed over the life of the contract shall meet all standards required for the applications the components will support (i.e., Federal Information Processing Standards (FIPS) 201 and FIPS 140.

Items that are used for DMDC applications dealing with PII or that fall under the Homeland Security Presidential Directive (HSPD)-12 regulations shall be purchased as in accordance with NIST and FIPS regulations and GSA's Approved Products List.

4.4.7 The Contractor shall store DMDC GFE and include maintenance coverage under the maintenance task when evaluation units are not readily available from manufacturers for testing and the components are purchased by DMDC for testing.

4.4.8 The Contractor shall provide system integration to the extent that all DMDC systems are shipped with as much of the system software pre-loaded on the hard drive, so that installers only need to perform a minimum amount of software installation and configuration once on-site. As much as possible, automated system software loads shall be used to establish the software baseline to ensure consistency of the produced baseline. The individual components and software shall be integrated, staged, and tested in the system configurations to be delivered. As patches/updates become available, integrate these into the load process. In addition, each system shipping to a site should include a print-out (from a system vulnerability scan) identifying compliance with all available IAVA patches, using DoD approved software. DMDC will provide all required application image CD-ROMs/DVDs and installation instructions to the Contractor for each system type.

4.4.9 The Contractor shall perform quality audits during integration and testing to ensure compliance with required service levels (see Appendix X). Upon completion of the test phase, systems shall be verified for completeness prior to shipment.

4.4.10 The Contractor shall provide boxes, packing materials, and shipping as required to move items between DMDC sites, the contractor, DMDC, and other locations designated by the Government. The Contractor shall maintain all DMDC provided site shipping addresses for hardware released in support of both fielding and maintenance activities. As new DMDC sites are added, DMDC will provide the initial shipping address. Shipping instructions are provided in PWS section 8.6.

4.4.11 Provide COTS Hardware and Software Engineering Support

4.4.11.1 The Contractor shall provide technical services to identify, test and document hardware and software.

4.4.11.2 The Contractor shall perform continuous COTS hardware and software market analysis to leverage current market trends and technology to ensure that the Government is able to procure all the COTS hardware and software components as detailed in Appendix K, "Technical Specifications for COTS for Hardware and Software".

4.4.11.3 DMDC requires end of life (EOL) notification on hardware components with projected end of life dates as far forward as possible. The Contractor shall monitor the components EOL at least quarterly basis and notify the government within 48 hours if given short notice from the manufacturer. As new technology becomes available, or the manufacturer's end of life approaches and products are discontinued, the Contractor shall propose upgraded or new hardware and software items via Engineering Change Proposals (ECPs), as defined below:

As a minimum, the following information shall be submitted with each ECP:

a. A discussion of what the proposed items will be used for.
b. A table depicting all of the current Government-provided technical specifications and original equipment manufacturers' (OEM) warranty for the current component comparing the previous product to the newly proposed product, with the make and model of each, any difference between the two products, and the comparative performance advantages and disadvantages of the newly proposed component compared to the current product.
c. For PCs and products that contain multiple pieces, the ECP shall include a Unique Identification Number and shall contain a list of all pieces by national stock number if available, description, make, model, warranty, price, Software and Hardware licensing/maintenance period of performance, and manufacturer part number that will be provided with the newly proposed CLIN (e.g., keyboard, mouse, hard drive, DVD/CD writer drive, extra batteries, cables, etc.).
d. All CLINs on the contractor's Hardware/Software Itemized List that are affected by the component change and if the new component will be a no cost substitution or require a new CLIN(s) to be created. If a new CLIN(s) is (are) required, the ECP shall include the new price(s) and warranty proposed.

e. Itemized requirements in the current Government-provided technical specifications that must be changed if the proposal is adopted, and the proposed revision to the technical specifications for each such change.
f. The contractor's rationale for selecting the proposed change, except in Government initiated changes.
g. An evaluation of the effects the proposed change would have on collateral costs to the Government, such as Government-furnished property costs, costs of related items, and costs of maintenance and operation.
h. Estimated manufacturer end of life and mean time between failures (MTBF) for the newly proposed product.
i. Provide proposed manufacturer's period of performance for COTS (e.g. software licenses 12 months).
j. A statement of the time by which the change order adopting the proposal must be issued, so as to obtain the maximum benefits of the changes during the remainder of the task order. Also, any effect on the task completion time or delivery schedule shall be identified.

Post award when changes to products occur, the Contractor shall provide via electronic media the supporting specification sheets and/or certification letters substantiating all of the technical specifications for each new item proposed to meet the Appendix K, Technical Specifications for COTS Hardware and Software.

Acceptance testing shall be considered an inherent step within the ECP process. Acceptance testing for all software and hardware replacement items shall be performed and submitted for each ECP in accordance with the Government-approved procedures in the Equipment Acceptance Test Plan, as discussed below:

The Equipment Acceptance Test Plan shall describe the contractor's procedures for acceptance testing of equipment procured and delivered under this PWS and for any equipment to be used as a replacement component, which differs from the baseline configuration. These acceptance procedures shall include how the contractor plans to verify that new items will properly operate under the latest version of the DMDC applications (i.e., RAPIDS, DBIDS, NTS, and/or JAMMS) operating systems, software applications, and other COTS software/drivers, as applicable. Appendix N, "DMDC COTS Acceptance Testing Methodology" shall be used as a guide to acceptance testing.

The Contractor shall provide an Equipment Acceptance Test Plan within 45 days of award.

4.4.11.4 The Contractor shall perform analysis of all COTS hardware and software in accordance with the Equipment Acceptance Test Plan discussed in PWS section 4.4.11.3. The Contractor shall demonstrate that all proposed hardware is compatible with the applicable existing DMDC system components and is capable of successfully running the applicable DMDC application software.

4.4.11.4.1 The Contractor shall provide capability to support remotely on BIOS system management for BIOS reset as required.

4.4.11.5 User Acceptance Testing

4.4.11.5.1 The Contractor shall participate in the User Acceptance Testing (UAT) of new software versions and components prior to the deployment in a production environment.

4.4.11.5.2 The Contractor shall participate in on-site reviews and beta test team meetings during UAT to analyze and document hardware and software performance.

4.4.11.6 Mobility Kit Redesign and Reengineering Support (for mobile kits): The Contractor shall propose new mobile kits redesign and reengineering to keep current with new technologies and changes in the system configuration. The kit design should consider ease of maintenance and the incorporation of technical changes while minimizing cost impacts.

4.4.12 Integration Test Lab

4.4.12.1 The Contractor shall provide the capability to evaluate, integrate and test DMDC applications with hardware platforms and hardware and software components, to include new or alternate operating systems, as requested by DMDC or customers to be provided DMDC applications. DMDC applications may utilize a number of software packages and peripheral devices, including printers, barcode scanners, biometric capture devices and various mobile devices (e.g., PDAs). This evaluation, integration and testing may be for integration of a single proposed component or an entire system including specific peripheral devices. The integration shall include application of all required security patches, version upgrades, and security lockdowns. The Contractor shall ensure the system and DMDC application is operational after hardware and software integration. The Contractor shall provide a report of evaluation and integration results and document all system changes and configuration required to integrate DMDC applications with the tested hardware and/or software.

4.4.12.2 The Contractor shall create and test automated deployment packages for DMDC applications or ancillary software/driver patches and upgrades.

4.4.12.3 The Contractor shall provide complete installation, operation and maintenance documentation for each integrated component or system. The Contractor shall prepare user install instruction hardware guides and tip sheets, and any other user documentation required to assist sites with proper installation, operation and maintenance of DMDC equipment provided under this Task Order.

As new technology becomes available or the manufacturer’s end of life approaches, the contractor shall update the Desktop and Deployable Hardware Guides as applicable for the new products and submit the updated Hardware Guide(s) to the COR and TPOCs within 20 working days after receipt of the new component for the contractor's lab in accordance with the format specified by the Government. The Government will provide the contractor with

the latest Desktop and Deployable Hardware Guides upon award, which are MS Word documents.

4.4.12.4 Hardware Test Report. As new technology becomes available or the manufacturer's end of life approaches, the Contractor shall perform acceptance test of new products within the DMDC applications hardware baselines and submit a Hardware Test Report to the COR and TPOCs within 5 working days after testing is completed in accordance with the format specified by the Government.

4.4.12.5 The Contractor shall review and provide material and feedback for all training materials as they relate to activities under this Task Order. Examples would include developing material for addressing frequently encountered errors, or proper usage instructions for operational maintenance of hardware components.

4.5 Worldwide COTS Hardware and Software Maintenance

The task requires that the contractor to provide maintenance of fielded equipment, maintenance solutions for worldwide DMDC supported applications/systems, trending analysis resulting in performance improvements, and warranty management.

4.5.1 The Contractor shall furnish the personnel, materials, shipping, tools, facilities, and personnel transportation necessary for performing worldwide remedial maintenance for DMDC sites.

4.5.2 The replenishment of any spare parts shall be proposed and purchased by the contractor at their discretion and shall be included in the fixed price maintenance cost. Repair service and repair parts/spare parts shall apply exclusively to the equipment types/models within the scope of this PWS.

4.5.3 Maintenance is inclusive of all software loads required to make the system operational, to include COTS software, latest applicable DMDC application software, latest patches/IAVA updates, download and installation of digital certificates, and any necessary hardware drivers applicable for the location where it will be operated. There are also cases where all troubleshooting attempts have been exhausted and reimaging of a device (e.g., computer, handheld) is required to provide expedient return of the system to operational status. Additionally, system security violations could potentially require the reimaging of a workstation prior to return and reactivation at a site.

4.5.4 Maintenance for an individual hardware component may be added or discontinued by the Government on thirty (30) calendar days written notice, or shorter notice when agreed to by the Contractor; such notice to become effective thirty (30) calendar days from the date on the notification. However, the Government may extend the original discontinuance date upon written notice to the Contractor, provided that such notice is furnished at least ten (10) calendar days prior to the original discontinuance date.

At the unilateral right of the Government, the Government may add GFE provided components not purchased under this task order for maintenance. These components would be of the same make or model available for procurement under this PWS. As required to support the DMDC infrastructure, other components for CLINs not available through for procurement through this PWS may be added as GFE for maintenance coverage through bilateral agreement.

4.5.5 The Contractor shall provide maintenance for all DMDC equipment listed in Appendixes D.3 "RAPIDS Fielded COTS Hardware", Appendix E.2, "DBIDS Hardware Equipment List", plus any additional components as requested by DMDC during the period of performance of this Task Order. Historical information is provided in Appendix R, "Call Volume Transferred to HW", and Appendix S, "HW SW Maintenance Calls by Region".

4.5.6 DMDC sites and equipment that are under maintenance shall continue to be maintained by the Contractor. For informational purposes, Appendix D.1 "RAPIDS – 2018 Site List" provides the current list of RAPIDS sites. Appendix D.2 provides a current RAPIDS World Map. A list of equipment, make and models currently fielded for RAPIDS is contained in Appendix D.3 "RAPIDS Fielded COTS Hardware" and Appendix D.4 "RAPIDS COTS Software". For additional RAPIDS Information reference Appendix D.5 through Appendix D.10.

Appendix E.1 "DBIDS 2018 Site List" provides the current DBIDS sites as well as the number of servers, workstations, and gates installed at each site that shall be maintained by the Contractor.

4.5.7 Consumable items such as toner cartridges and batteries shall be disposed of by the on-site POC. DMDC does not normally supply the sites with replacement toner cartridges. These would only be replaced if the maintenance technician determined that the original toner cartridge was defective during an on-site maintenance call or a site is provided an alternate brand of printer as a maintenance replacement. The Contractor shall follow the appropriate rules and regulations for the disposal of such consumable items and HAZMATs.

4.5.8 Equipment placed under maintenance service shall be in good operating condition. In order to determine that the equipment is in good operating condition, the equipment shall be subject to inspection by the contractor, without charge to the Government. Ensure equipment is in proper operating condition.

4.5.9 Government personnel will not perform maintenance or attempt repairs to equipment while such equipment is under the purview of the maintenance task under this PWS, unless agreed to by the Contractor. Subject to security regulations, the Government will permit access to the equipment, which is to be maintained or repaired. All parts, furnished as spares or as repair parts in connection with the repair of equipment, unless otherwise indicated in this PWS, shall be new, standard parts manufactured by the original equipment manufacturer.

4.5.10 The Contractor shall be responsible for any damage or loss of equipment, from the time the equipment is removed from the Government installation, until the equipment is returned to such installation or GFE storage.

4.5.11 The Contractor shall provide detailed packing and shipping instructions to users for equipment returns. Any equipment received by the Contractor that is damaged due to user mishandling or abuse must be reported to the Government within 14 days of receipt.

4.5.12 Whenever maintenance actions require that equipment be excessed to a site, the Contractor shall provide the site POC with a pre-filled Requisition and Invoice/Shipping Document (Department of Defense [DD] Form 1149) for signature, documenting the serial numbers of the equipment being excessed to the site. The Contractor shall request that the DD Form 1149 be signed by the site POC and returned or sent by facsimile (FAX) to the Contractor, for updating the Configuration Management Database that is established and maintained by the Contractor. The Contractor shall notify the applicable DMDC program office of sites that do not comply with returning the signed DD Form 1149 to the Contractor within two (2) weeks. Whenever a computer (server, workstation, laptop/notebook, or handheld computer) is being excessed, ensure that a DoD-approved disk wipe/memory wipe has been performed before excessing it to the site or shall arrange for the computer to be returned to the Contractor's facility to be wiped.

4.5.13 All user calls are initiated through the DMDC Customer Contact Helpdesk. After initial troubleshooting, unresolved hardware and installation-related calls will be forwarded to the Contractor for action. The Contractor's maintenance solution should include automated interface to DMDC's Customer Contact Helpdesk ticketing system. Currently, that system is operating with CA Service Desk Manager.

4.5.13.1 All maintenance actions shall be initiated only after the Contractor receives notification from DMDC or the Customer Contact Helpdesk specifying a hardware failure. A call is the initiation of work to be performed at a problem location. Maintenance service level requirements are provided in Appendix X, "Performance Requirements Summary".

4.5.13.2 For all maintenance calls, the Contractor shall annotate in the DMDC Customer Contact Helpdesk ticketing system all actions taken and notify the notify the Helpdesk to close the trouble ticket once the downed site is confirmed as operational. If a call cannot be closed in the negotiated response time, the Contractor shall notify DMDC in the Weekly Maintenance Open Call Report described below:

All maintenance actions that remain open after two (2) business days from when the call was opened (may be negotiated to one (1) day for DBIDS) will be documented in the Weekly Open Call Report. This report should be presented by program (RAPIDS, DBIDS, etc.), electronically in MS Excel format and provide the following information at a minimum:

a. The forwarding support center provided trouble ticket number;
b. The site number, site name, and address;
c. The Site POC and phone number;

d. Date/time of notification to perform maintenance (when the call was opened with the contractor);
e. Description of the problem provided by the forwarding support center;
f. Description of the problem found by the contractor maintenance personnel and service action taken;
g. List of all parts shipped to site for repair and date shipped;
h. Description of type of service: on-site or mail-back; and
i. Detailed explanation for why the call is not closed.

4.5.14 The Contractor shall perform maintenance for all indicated equipment at a fixed monthly rate. This fixed rate pricing model shall take into account maintenance management, maintenance activities, warranty, travel, two-way shipping costs, packaging costs, repairs, spare parts and any other items the contractor deems required to provide maintenance in accordance with Appendix X, "Performance Requirements Summary". On a quarterly basis, deliver an analysis of the support; as required, cost adjustments will be negotiated to the fixed monthly cost to accommodate increases or decreases from the established quantity of components for warranty and maintenance of specific items. Adjustments will be made using the actual prices proposed for the warranty/maintenance per item.

4.5.15 The Contractor shall define the warranty to be provided for new hardware purchased under their proposal and in all engineering change proposals to that initial equipment list. The cost to purchase each COTS hardware item should include the warranty proposed at no additional cost to the Government. In addition the following subparagraphs apply to the warranty as it relates to the Maintenance task for this PWS:

4.5.15.1 The Contractor shall coordinate all warranty maintenance actions, from initial installation through expiration of the original equipment manufacturers' (OEM's) warranty period. The warranty period shall begin at time of equipment installation. Warrant and imply that the items delivered hereunder are merchantable and fit for use for the particular purpose described in this PWS.

4.5.15.2 Prior to the expiration of the OEM's warranty period, whenever equipment is shipped for mechanical replacement purposes, shipping costs shall be the responsibility of the Contractor to include the cost of packing, transportation, rigging, drayage, and insurance. The labor costs associated with the diagnosing and replacing of a component that fails prior to the expiration of the OEM's warranty period will not be the responsibility of the Government.

4.5.15.3 The Contractor shall be responsible for all remaining OEM warranties for fielded and/or purchased GFE under this PWS. For informational purposes, Appendix L, "DMDC Equipment Warranty Status" provides a list of DMDC components still under warranty and those out of warranty.

4.5.16 The Contractor maintenance solution for world-wide DMDC sites shall ensure that the necessary AQLs are met (see Appendix X – Performance Requirements Summary). The

Contractor's solution may include mail-back maintenance, especially for remotely located OCONUS sites, which cannot cost effectively be provided on-site maintenance support within the specified response time defined in the AQL. Generally, maintenance for portable systems deployed in the field, including NTS/ETAS, and RAPIDS deployed and on-board U.S. Navy ships, will be performed via mail-back maintenance to the site location where the systems were deployed. For RAPIDS and DBIDS, all CPU repairs should be performed on-site (any exceptions for remote or deployables shall be identified to the DMDC POC prior to execution). The cost of all shipping for maintenance shall be included in the Contractor's firm fixed price.

4.5.16.1 If mail-back maintenance is used, and the Contractor does not receive confirmation back from the DMDC site after 3 attempts or the site refuses to perform the maintenance, the Contractor shall notify the applicable DMDC program office for assistance.

4.5.17 Quarterly Maintenance Rate

4.5.17.1 The time for each quarter under this PWS will begin on the first day of the month of the Task Order award.

4.5.17.2 Each quarter, the Contractor shall provide an analysis of all changes to the configuration baseline over the preceding quarter to include, at a minimum, changes for in/out warranty, excess equipment, and labor requirements.

4.5.17.3 The Contractor shall submit their cost analysis to the COR on the 5th business day of the last month of the quarter. The Government will provide approval or changes back to the contractor within five (5) business days after receipt. Upon notification of changes from the Government the Contractor will have five (5) business days to make any changes/corrections and resubmit to the Government. Upon acceptance and approval by the Government a modification to incorporate the quarterly rate adjustment into the Task Order will be issued.

4.5.17.4 The new Quarterly Maintenance Rate will become effective on the first day of the month for the first month of each quarter.

4.6 Integrated Program Management System (IPMS)

In this task, the Contractor shall stand up an IPMS that meets or exceeds the NIST 800-171 Rev 1 – Protecting Controlled Unclassified Information (CUI) in Non-Federal Systems and Organizations that provides recommended requirements to process, store, transmit CUI or providing security protection of the IPMS. As part of task order transition, existing IPMS data will be transferred from the incumbent to the incoming contractor.

4.6.1 The Contractor shall furnish everything required to meet the service level requirements as outlined in Appendix X, "Performance Requirements Summary" which contains the Acceptable Quality Levels (AQLs), and to incorporate Government property accountability and management (DoD Instruction 5000.64) rules and regulations. DMDC

supports a number of projects and application users that require property and configuration management, to include: RAPIDS, DBIDS, NTS/ETAS, and JAMMS. Minimum data requirements are provided in Appendix J, "Configuration Management System Fields and Reports".

4.6.1.1 The Contractor shall track components throughout their life cycle by serial number starting when they are received by the Contractor and until they are no longer used and are excessed through proper Government channels. The Contractor shall maintain accurate inventory information in accordance with DoD property accountability regulations (i.e., DoD Instruction 5000.64, Accountability and Management of DoD Equipment and Other Accountable Property). The inventory and related reports shall be made available to all DMDC designated personnel located both at DMDC offices and remotely worldwide.

4.6.1.2 When equipment is at the Contractor facility, it should be recorded in the configuration management database for full tracking while in the contractor's possession to maintain chain of custody.

4.6.1.3 The Contractor shall establish, implement and maintain a Configuration Management Database system. The Contractor's configuration management system shall be capable of providing secure, on-line, up-to-date configuration management data to the Government (including worldwide application users) via the World Wide Web. The Contractor's solution shall be role-based and shall provide the capability for DMDC users, which include personnel on other contract vehicles, to query individual records, run defined reports, and construct ad hoc reports containing records and data elements selected by the DMDC user. The Contractor's solution shall provide the capability to display reports on the DMDC user's PC screen, export them in MS Excel format, and print them to their local printer.

4.6.1.4 The Contractor shall prepare the Assessment and Authorization artifacts for the Contractor's configuration management system and shall work with DMDC to obtain the requisite RFM certification.

4.6.1.5 The configuration management system shall use CAC authentication (Public Key Infrastructure (PKI) as the primary user identification.

4.6.1.6 Data fields shared with DMDC's DEERS database and another DMDC Contractor's helpdesk ticketing system shall be maintained in the same data format to ease import into the configuration management system. These shared fields are indicated with an asterisk (*) or plus (+) in Appendix J, "Configuration Management System Fields and Reports". The configuration management system shall accept electronic updates via email or web and provides its updates to DEERS and the ticketing system databases nightly or within 24 hours of when updates occur. Over the course of the task order the interfaces to DMDC may change in order to access data and interfaces to other systems may be added. DMDC will work with the contractor on the requirements as they arise.

4.6.1.7 The configuration management system shall include Site and System Inventory and Configuration Data for existing and newly procured COTS software and hardware at existing and new DMDC sites. The Contractor shall update configuration management records to account for all receipts of equipment by the Contractor and for all system installations, system relocations, system de-installations, and maintenance actions. This includes those provided by the Contractor, as well as other DMDC support contractors. The Contractor shall maintain site, system inventory, and configuration data for each DMDC site and individual systems/components as applicable. The configuration management system shall provide data retrieval by user-defined query. The Government will provide updates to site names, DEERS site IDs, POCs, addresses, phone numbers, and FAX numbers as they become known. Any data discrepancies or updates of fields where DEERS and the helpdesk ticketing system databases are the master source should be reported to the Government as soon as found for expedient resolution. The Contactor shall obtain and maintain current shipping addresses for hardware released in support of both fielding and maintenance activities at DMDC sites. The current Site and System Inventory and Configuration Data fields and reports are detailed in Appendix J, "Configuration Management System Fields and Reports".

4.6.1.8 The Contractor shall provide CLIN Data for all COTS hardware and software available on the contractor's hardware/software itemized pricing list for purchase in accordance with Appendix K - Technical Specifications for COTS Hardware and Software. The configuration management system shall provide CLIN data retrieval by user-defined query. The report to be provided to the Government monthly and available for download any time will be contained in the Appendix T, "COTS Hardware/Software Cost Table Template" (to be provided at award). The current CLIN Data fields and reports are detailed in Appendix J, "Configuration Management System Fields and Reports" and are subject to change.

The Contractor shall create and maintain the Consolidated Equipment Summary. The format will be approved by the Government. The Contractor shall update the summary whenever the contractor makes a change to any of the CLINs on their hardware/software itemized pricing list for use by DMDC applications and as a minimum at least monthly. Whenever the summary is updated, the Contractor shall submit this report electronically in MS Excel format. Whenever a CLIN change is made, the contractor shall notify the COR and TPOCs via e-mail with the date the change becomes effective and the applicable task order Modification (Mod) number.

4.6.1.9 The Contractor shall provide COTS Hardware and Software Technical Requirements (from Appendix K, "Technical Specifications for COTS Hardware and Software"), Market Surveys, and Evaluation Score Sheets (Appendix W). The Contractor shall enter market survey results for newly proposed makes/models completed against the mandatory technical requirements. The system will be capable of exporting the market surveys and evaluation score sheets to MS Excel for review by the DMDC and other support contractors. The DMDC shall have on-line access to update/maintain the technical specifications, market survey fields and data, and evaluation score sheet fields and data in the configuration management system on-line. Other DMDC support contractors will have on-line access to the evaluation score sheets to enter their scores.

4.6.1.10 The configuration management system shall also include Site Action Schedules for the following actions to be performed by the contractor: site surveys, system installations, system relocations, and system de-installations, unless otherwise directed by DMDC.

4.6.1.10.1 The configuration management system shall include Site Configuration data to include site network information, workstation and device network and configuration information, workstation and device certificate management information, and site and device encryption parameters. Site configuration data shall be maintained for each site action that is to be performed by the contractor.

4.6.1.10.2 Site action schedule data shall be maintained for each site action that is to be performed by the contractor. The system shall provide data retrieval by user-defined query. The site action schedule data fields and reports are detailed in Appendix J, "Configuration Management System Fields and Reports".

4.6.1.10 The Contractor shall update configuration data in the database no later than two (2) weeks following their occurrence.

4.6.1.11 The Contractor staff shall perform the following activities:

a. During transition, the Contractor shall interface with the existing DMDC Integrated Program Management System (DIPMS) database and server running Structured Query Language (SQL)*Server with Crystal Reports until the Contractor's configuration management solution is operational and base lined.

The Contractor shall design, develop and implement the Contractor's configuration management solution as proposed and agreed to by DMDC. The Contractor shall provide a plan to achieve inventory baseline within 3 months of award, data accuracy within 4 months of award, and a technology roadmap including milestones and schedules. At a minimum, the roadmap shall include a plan that forecasts products' lifecycle and emerging technology. The plan shall provide a schedule for replacements and upgrades while optimizing capability and total cost of ownership.

b. The Contractor shall maintain the currency of data in the configuration management system via data input by the Contractor and data feeds from other DMDC databases. Automation of data entry is encouraged where possible to expedite entry/updates, reduce typographical errors, and ensure data consistency.

c. Upon completion of each site activity and maintenance action, the Contractor shall enter and update all applicable site, inventory and configuration data in the Configuration Management Database in accordance with Appendix X, "Performance Requirements Summary". If the Contractor is unable to obtain any third party data (e.g., from sites for mail-back maintenance or self-help relocations, etc.) within 2 weeks following the action

completion date, the Contractor shall notify the applicable DMDC program office of the outstanding data.

d. The Contractor shall conduct periodic audit checks to ensure database accuracy in accordance with the performance metrics.

e. The Contractor shall create, maintain, and provide all requested reports from the configuration management system. The current list of reports is included in Appendix J, "Configuration Management System Fields and Reports".

4.6.2 Asset/Inventory Management

4.6.2.1 The Contractor shall ensure the IPMS is updated to properly reflect the current configuration of all sites requiring support. Whenever possible these updates shall be made real-time. Due to the location of some of our sites, installation data should be updated no later than 14 days of the completed installation unless otherwise approved by the Government based on specific site communications issues.

4.6.2.2 DD Form 1149's for specific site hardware and site inventory lists shall be readily available to be produced on the system and delivered upon request.

4.7 TRANSITION

A smooth transition between the incumbent contractors and successor Contractor is necessary to ensure there is no disruption to vital Government business. To minimize risk during transition, the offeror will be required to propose costing for the existing products (same make/model) currently being fielded. This will ensure DMDC has orderable systems until such time as the contractor's alternate solution is approved via acceptance testing.

The contractor's transition plan shall provide sufficient detail to ensure an orderly transition can occur by that date minimizing the cost to the Government for concurrent costs. The Contractor shall cooperate fully in the transition.

Transition-In
The contractor has several requirements that shall be completed in order to effect a successful transition of the work from the existing contracts to the new task order.

4. 7. 1. The Contractor shall:

- Initiate paperwork required to support Status of Forces Agreement (SOFA)/ Technical Expert Status Accreditation (TESA)/Theater Business Clearance (TBC) and Foreign Clearance Guides. The Contractor will work with the Government PM/representative for the TESA system, who will create accounts for applicants wishing to receive SOFA status.
- Make sure that the contractor personnel meet the required Security and Credentialing requirements
- Work with DMDC to coordinate required interfaces to DMDC and ensure ability to obtain RFM certification of their solutions if they are touching DMDC network

4.7.2. The Contractor shall accomplish the following for each task:

- 4.1 – Worldwide Site Management Support: All subtasks will require a knowledge transfer, application certification training.
- 4.2 – Worldwide Communication Engineering Support: All subtasks will require knowledge transfer and training. The contractor shall have a solution in order to allow its personnel to view the network to proactively work with our users.
- 4.3 – Outside the Continental United States (OCONUS) Support: All subtasks will require knowledge transfer, application certification training,
- 4.4 – COTS Hardware and Software Support: All subtasks shall require a GFE transfer from incumbent and stand up of an Integration Test Lab with DMDC interface. All new hardware, not currently "qualified" to work in DMDC application suites, will require integration/acceptance testing by the Government. The contractor shall provide the makes/models of any new hardware and provide loaners whenever possible for testing purposes. To minimize risk during transition, the offeror will be required to propose costing for the existing products (same make/model) currently being fielded in addition to any new products they would like to propose. This will ensure DMDC has orderable systems until such time as the contractor's alternate solution is approved via acceptance testing. The length of transition time and the requirement to continue to order existing products will be dependent on the number of new components offered and the extent of the integration efforts required.
- 4.5 – Worldwide COTS Hardware and Software Maintenance: The contractor shall stand up a Tier 3 helpdesk and work with DMDC and DMDC Customer Contact Center to establish call transfer procedures and interface requirements between systems (dependent on contractor's solution)
- 4.6 - Integrated Program Management System (IPMS) – Development of a new IPMS solution. The Contractor shall obtain a RFM and NIST 800.10 certification, interface with other DMDC systems, and the transition of data from the current system to this solution to maintain all historical data.

4.7.3 The Contractor shall submit a final Transition Plan within 30 days after task order award addressing the following:

- Transition of the DMDC initiatives to ensure a smooth transition from task performance under the incumbent contractor to task performance under the offeror's program management and task performance.
- Proposed sequence of transition tasks, which should be accomplished to progress from project start to fully effective performance of the tasks, specified in the PWS.
- Maintaining DMDC schedule, specifically transition of existing, on-going efforts and concurrently working with incumbent on existing efforts.
- Obtaining SOFA Status and Theater Business Clearance (TBC)
- Time and process to stand up the contractor's maintenance system to include helpdesk interface with the DMDC Customer Contact Center and worldwide spares readiness.
- Schedule to migrate the configuration management system to a web-based application.
- Proposed process for GFE transfer from the incumbent contractor to the offeror.

- Stand up acceptance test lab.
- Controlling costs and maintaining schedule.
- Identification of associated risks and issues.
- Risk Mitigation strategies to address any risk issues.
- Resources required for the transition.
- How transition will be implemented and managed.
- Problems anticipated.
- Past experience the offeror had in transitioning project(s) comparable in scope, size and complexity.
- Transition planning for Contract close out.

Ensure that all hardware/software agreements entered into under WWHWSW I contract are transferred to WWHWSW II.

Transition-Out

The contractor shall provide a written Transition-Out plan NLT 180 days prior to expiration of the task order, or earlier if directed by the Government. The Transition-Out plan shall facilitate the accomplishment of a seamless transition from the incumbent to incoming Contractor/Government personnel at the expiration of the task order. Within the plan, the contractor shall identify how it will coordinate with the incoming Contractor and/or Government personnel to transfer knowledge regarding the following:

- Project management processes
- Points of contact
- Location of technical and project management documentation.
- Status of ongoing technical initiatives
- Technical artifacts and configuration baselines
- Transfer of portal data
- Appropriate contractor-to-contractor coordination to ensure a seamless transition
- Transition of personnel
- Identify schedules and milestones
- Identify actions required of the Government
- Establish and maintain effective communication with the incoming Contractor/Government personnel for the period of the transition
- Inventory of assets and transfer of government furnished equipment, i.e. software and hardware, licenses, warranties, etc.
- System administration, accounts, privileges, and accesses
- Existing leases and rental contracts for such things as office space, apartments, rental vehicles, etc.

4.8 OPTIONAL TASKS

The options described below will be invoked through award of a written task order modification issued by the GSA Contracting Officer (CO). Options may be invoked, in whole or in part, at the discretion and unilateral right of the Government.

4.8.1 OPTIONAL TASK 1: SURGE CAPABILITY

The Government reserves the unilateral right to exercise Optional Surge Capability to support unforeseen, ad hoc requirements or unplanned increases in workload that may arise under the scope of this PWS. Optional surge capability support will be invoked at the Government's discretion through a written task order modification issued by the GSA Contracting Officer.

For pricing purposes, the Not-To-Exceed (NTE) ceiling amount established for this Optional Surge Capability in each year of performance is shown in the table below:

Base Year NTE	Option Year 1 NTE	Option Year 2 NTE	Option Year 3 NTE	Option Year 4 NTE
$4,600,000.00	**$4,600,000.00**	**$4,600,000.00**	**$4,600,000.00**	**$4,600,000.00**

For proposal purposes, contractors shall include pricing for a labor mix with CONUS and OCONUS labor rates to support surge capability requirements as shown in the pricing template.

Prior to awarding the modification, the Contracting Officer will provide the Contractor with a written request for surge capability specifying the unforeseen, ad hoc or unplanned increases in workload support required, the nature of work to be performed, deliverables, and required timeframes. The Contractor shall respond to this request in writing within five (5) business days with a quote showing the proposed staffing plan and notional schedule to meet the government's requirements. Generally, the Contractor shall have the capability to surge contractor staff to meet mission demands within 30 calendar days of the effective date of the modification; however there may be a need to begin a surge effort within a shorter response time. The Contractor shall manage workload surges effectively and in a manner that efficiently schedules and applies contractor resources to meet mission requirements and DMDC priorities. The Contractor shall meet the surge capability requirements without decreasing the current support to, or quality of, any of the other DMDC requirements under this task order.

The Contractor shall coordinate with the Government to plan and adjust staffing schedules to support surge capability activities while concurrently delivering ongoing services, without degradation, for day-to-day operations under the scope of this PWS. This may include adjusting normal work schedules, backfilling positions, or minimizing/prohibiting leave of individual Contractor employees to achieve the required coverage.

4.8.2 OPTIONAL TASK 2: ENTERPRISE SUPPORT CAPABILITY

During this Task Order, it is anticipated that DMDC may require additional enterprise-wide COTS hardware, software, maintenance, and integration services in the base and each option year to be exercised as a unilateral right of the Government. As such, the Government reserves

the unilateral right to exercise Optional Enterprise Support Capability for applications and systems that leverage data holdings, whereby DMDC requires services similar to the scope of PWS Sections 4.1 through 4.6 if/when assuming responsibilities for the control and support of additional applications or systems pursuant to PWS Sections 3.3 and 3.4. This optional work may be exercised on a firm fixed price or labor hour basis.

For pricing purposes, the Not-To-Exceed (NTE) ceiling amount established for this Optional Enterprise Support in each year of performance is shown in the table below:

Base Year NTE	**Option Year 1 NTE**	**Option Year 2 NTE**	**Option Year 3 NTE**	**Option Year 4 NTE**
$8,00,000.00	**$8,000,000.00**	**$8,000,000.00**	**$8,000,000.00**	**$8,000,000.00**

For proposal purposes, contractors shall include pricing for a labor mix with CONUS and OCONUS labor rates to support enterprise positions for PWS tasks 4.1-4.6 as shown in the pricing template.

For any optional task support that the Government invokes pursuant to PWS Sections 3.3 and 3.4, the Government will specify the applications and systems that require support; the duration for the support; the CONUS and OCONUS location(s) where support is required; reporting requirements; and work hours, schedules, or requirements for performing work outside of normal working hours (i.e. evenings, weekends, etc.).
The scope of this optional enterprise support capability will be specified in technical direction letters and may span requirements described in PWS Sections:

- 4.1 Worldwide Site Management Support
- 4.2 Worldwide Networks and Communications Engineering Support
- 4.3 Outside the Continental United States (OCONUS) Support
- 4.4 COTS Hardware and Software Support
- 4.5 Worldwide COTS Hardware and Software Maintenance
- 4.6 Integrated Program Management System (IPMS)

At the time of exercising this optional support, the Contracting Officer will issue technical direction that defines the specific systems where optional services are required:

- Identify the specific location(s) and to be supported;
- Provide technical direction necessary to clearly delineate extent of support and nature of work to be performed, deliverables, and required timeframes, if any;
- Specify the IPMS and configuration management requirements;
- Identify any elevated service level or response time requirements, if any;

- Delineate training requirements, desired outcomes, extent and nature of any knowledge transfer activities for maintainer and/or end-user training to be conducted; and training documentation or related materials required of the Contractor, if any.
- Specify the background investigation or security clearance requirements, if any; and
- Define working hours and where applicable, any site unique conditions associated with this support.

The Contractor shall respond to this technical direction letter in writing within ten (10) business days with a proposal showing the proposed staffing plan to meet the government's requirements.

Contractor personnel shall meet the applicable certification requirements of DoD Manual 8140.01, Cyberspace Workforce Management, as noted in PWS Section 12.0.

When optional work is exercised, the services rendered under this optional task shall be documented and reported in Monthly Progress Reports and progress updates, performance metrics, and status on such work shall be covered in program reviews/technical interchange meetings consistent with technical/program management activities described in PWS Section 4.1.

The Contractor shall maintain chain of custody and accountability for any GFE/GFP/GFI provided under the scope of this optional task consistent with the PWS Section 9.0 and the IPMS requirements defined in PWS Section 4.6.

5.0 DELIVERABLES

PWS Reference	Deliverables	Date Due/Frequency
4.1.4.3.1	Monthly Progress Report	20th workday of every month
4.1.4.3.2	Technical Report/Study	As requested
4.1.4.3.3	Senior Management Review (SMR)	Three (3) business days in advance of the meeting
4.1.4.3.4 4.1.9	Meeting Minutes	Three (3) business days after the meeting
4.1.4.3.5	Meeting Agenda	Three (3) business days in advance of the meeting
4.1.4.3.6	Risk Mitigation Plan	Within 30 business days after award (submit with Transition Plan). Subsequent Plan changes within five business days of updates being finalized
4.1.4.3.7 and Appendix	Contract Discrepancy Resolution Report	Within 5 business days from date of identification/discovery

AB		
4.1.4.3.8	Technology Road Map	3 months after Task Order Award and 60 days after award of each option
4.1.5.1	Site Survey Report	No later than 2 weeks after completion of site survey
4.1.7.4	Training Checklist	Within fourteen calendar days of the visit
4.1.9	Reports, Studies, Invoices, Schedules	As directed by DMDC
4.1.9.9	Monthly RAPIDS User/Non-Compliance (SSM/VO) Report	Within the first 5 business days of each month using data pulled on the first business day of each month
4.1.9.9	Quarterly RAPIDS Workstation Utilization Report	Within 5 business days of receipt of the data
4.1.9.9	Annual RAPIDS Workstation Allocation Review Spreadsheet	Six weeks prior to date of workstation allocation review meeting
4.1.9.9	Monthly CAC Failure Report	Within 5 business days of receipt of the data
4.1.9.10 4.1.9.11	Standard Operating Procedures (SOPs)	As specified. Reviewed for required updates annually
4.2.6.5	Vulnerabilities Report	Weekly, due by close of business each Monday
4.2.6.6	POA&M Tracking Report	Weekly
4.2.6.7	HBSS Report	Weekly
4.2.6.10	Workstation Connectivity Report	Weekly
4.2.6.10	Monthly Security Compliance Report	Monthly
4.3.7.1	Test Plan and Test Results	As required
4.4.1.1	COTS Renewal Report	Quarterly
4.4.11.4	Equipment Acceptance Test Plan	Within 45 days of award
4.4.11.4	Engineering Change Proposal	As required or within 30 days of updated technical specification
4.4.12.3	Hardware Guides	Within 20 working days after receipt of new component for the contractor's lab
4.4.12.4	Hardware Test Report	Within 5 working days of testing

4.5.14.2	Weekly Maintenance Open Call Report	After maintenance action have been open for more than two business days
4.5.18	Quarterly Maintenance Rate	The first day of the month in each quarter
4.6.1.7	Consolidated Equipment Summary	Whenever a change is made to a CLIN
4.7.3	Transition Plan	30 days after task order
6.3	Quality Control Plan	Within 30 days of award
8.6.6	Government Shipping Account Usage Report	Monthly

6.0 QUALITY ASSURANCE

6.1 Quality Assurance Surveillance Plan (QASP). The Government intends to utilize a Quality Assurance Surveillance Plan (QASP) to monitor the quality of the Contractor's performance. The oversight provided for in the order and in the QASP will help to ensure that service levels reach and maintain the required levels throughout the contract term. Further, the QASP provides the COR with a proactive way to avoid unacceptable or deficient performance, and provides verifiable input for the required Past Performance Information Assessments. The QASP will be finalized immediately following award and a copy provided to the Contractor after award. The QASP is a living document and may be updated by the Government as necessary. The Government will also review the Monthly Progress and Quality Reports and will attend regular work performance review meetings with the Contractor to survey quality of products and services.

6.2 Quality Control and Assurance

6.2.1 The Government reserves the right to perform inspections and surveillance to evaluate the Contractor's compliance to the contract terms and performance of the requirements in the PWS. The Government will make every effort to ensure that the surveillance methods described below are conducted in an objective, fair, and consistent manner. Appendix X provides the Performance Requirements Summary and identifies the critical performance elements, performance standard, and acceptable quality levels (AQLs).

6.2.2 Periodic Surveillance: This action occurs when the COR or other Government official observes a deficiency. Examples include evidence from accidents, incidents, or delays. Regardless of where in the line-of-duty the COR observes contractual procedures not being followed, he/she has an obligation to document and report the deficiency to the Contracting Officer.

6.3 Quality Control Plan. The Quality Control Plan (QCP) is the contractor's internal plan to insure quality delivery of products and services under the terms of this Task Order. The QCP

should detail the contractor's internal controls for services under this Task Order and should have a direct relationship to the proposed terms of the QASP. The Contractor shall implement and maintain a QCP to ensure work performed conforms to the scope of work and meets the requirements under this PWS. The QCP shall, at a minimum provide a method for performing inspections; identifying, correcting and preventing problems/defective service; addressing customer complaints, and improving the quality of services over the life of the Task Order. The contractor will submit their QCP to the Government within 30 days after award.

6.4 Requirements Summary: Within Appendix X - Performance Requirements Summary, the Contractor service requirements are summarized into performance objectives that relate directly to mission essential items. The performance threshold briefly describes the minimum acceptable levels of service required for the significant performance requirements of this Task Order. These thresholds are critical to mission success. The Contractor shall ensure its performance under this Task Order meets the quality standards identified in the Performance Summary Requirements.

6.5 Performance Evaluation Process: The Contractor Performance Assessment Reporting System (CPARS) has been adopted by Government to electronically capture assessment data and manage the evaluation process. CPARS is used to assesses a Contractor's performance and provide a record, both positive and negative, on a given contract/Task Order during a specific period of time. The CPARS process is designed with a series of checks and balances to facilitate the objective and consistent evaluation of Contractor performance. Both Government and Contractor program management perspectives are captured on the CPAR form and together make a complete CPAR. Once the Assessing Official completes the proposed assessment for the period of performance, the CPARS is released to the appropriate Government Contractor Representative for their review and comments. User ID and Password will be provided to the designated Government Contractor Representative upon issuance of a task order. The Contractor has 30 days after the Government's evaluation is completed to comment on the evaluation. The Government Contractor Representative must either concur or non-concur to each CPAR. If the Contractor concurs with the proposed assessment and the Reviewing Official does not wish to see the CPAR, the Assessing Official may close out the CPAR. Otherwise, they must forward the CPAR to the Reviewing Official for them to review, enter comments if appropriate, and close out. The Reviewing Official may at their option direct the Assessing Official to forward every CPAR to them for review.

7.0 INSPECTION, ACCEPTANCE AND PAYMENT

The Government will designate officials who have been delegated specific technical, functional and oversight responsibilities for this Task Order. The designated officials are responsible for inspection and acceptance of all services, incoming shipments, documents and services.

7.1 Delivery Address. All deliverables shall be submitted to the designated DMDC POC's. Additionally, the Contractor shall upload the deliverables into the GSA ITSS Portal unless directed otherwise.

7.2 Method of Delivery. The Contractor shall provide all deliverables and reports in PWS Section 5.0, the format of which to be defined or approved by the Government and subject to change over the course of the task order.

7.3 Acceptance Criteria. Acceptance by the Government of satisfactory services provided in contingent upon the Contractor performing in accordance with the performance standards contained in the Appendix X - Performance Requirements Summary and all terms and conditions of this Task Order, including all modifications.

7.4 Acceptance of Deliverables. The Government has 15 calendar days to review any draft documents and notify the contractor of approval or recommended changes to be made in the final version. If the Government does not provide an approval within the 15 days, the Contractor shall not assume that the deliverable is accepted by the Government. The contractor shall request a status update from the GSA COR. Final deliverables are then due within 10 working days after receipt of any Government comments on the draft. The Government COR has the final determination as to the format and the method that deliverables are submitted.

7.5 Invoicing and Billing

The Contractor shall submit Requests for Payments in accordance with requirements below. The Contractor shall provide invoice backup data in accordance with the contract-types established on this Task Order, including detail such as labor categories, rates and quantities of labor hours, and itemized travel, ODCs/Incidentals, maintenance rates, etc.

The Government reserves the right to audit, thus; the Contractor shall keep on file all backup support documentation for labor, travel, ODCs/Incidentals, and quarterly maintenance rate adjustments, etc.

The Contractor shall submit a draft or advance copy of an invoice to the DMDC client POC for review prior to submitting such invoice to GSA for payment per PWS section7.5.2 Invoice Submission Process instructions. The Government reserves the right to require certification by a GSA COR before payment is processed.

7.5.1 Invoice Requirements

The Period of Performance (POP) for each invoice *shall* be for one calendar month. The contractor *shall* submit only one invoice per month per order/contract. The appropriate GSA office will receive the invoice by the twenty-fifth calendar day of the month after either:

(1) The end of the invoiced month *(for services)* or
(2) The end of the month in which the products *(commodities)* or deliverables (fixed-priced services) were delivered and accepted by the Government.

For Labor Hour and Time and Material orders/contracts each invoice shall show, the skill level category, the hours worked per skill level, the rate per skill level and the extended amount for that invoice period. It *shall* also show the total cumulative hours worked (inclusive of the current invoice period) per skill level, the hourly rate per skill level, the total cost per skill level, the total travel costs incurred and invoiced, and the total of any other costs incurred and invoiced, *as well as* the grand total of all costs incurred and invoiced.

Firm Fixed Price CLINs
On the monthly invoice, Firm Fixed Price (FFP) CLINs shall be billed on the basis of 1/12th of the overall Firm Fixed Price (FFP) established for the CLIN. The monthly FFP shall be pro-rated equitably if a partial month or performance period of less 12-month in duration is encountered.

On monthly invoices, the Contractor shall apply the appropriate maintenance rate consistent with PWS 4.5.18 and the quarterly rate adjustment incorporated by the Contracting Officer into the Task Order.

Labor Hour / Time and Material CLINs For Labor
On the monthly invoice, Labor Hour / Time and Material CLINs shall billed on the basis of costs incurred for the Labor CLINs. All hours and costs shall be reported to the individual contractor employee level, and shall show the current charges for the month and cumulative totals for the period. The Contractor shall provide the invoice data on separate worksheets in the spreadsheet with the following detailed information. The listing shall include separate columns and totals for the current invoice period and the order to date and include:

a. Employee name (current and past employees)
b. Employee company labor category
c. Employee Alliant labor category
d. Actual Hours worked during the monthly billing period and total cumulative hours worked
e. Current costs billed and cumulative costs

Travel
The Contractor shall adhere to FAR part 31.205-46 for travel associated with this contract. This shall include all travel requirements associated with temporary duty (TDY) or deployments as required under this task order, Contractor personnel are authorized to invoice travel related costs at the allowance referenced in FAR part 31.205-46. For travel procedures, refer to PWS Section 8.7.

Cost incurred for Travel shall be shown on the monthly invoice with travel itemized by individual and trip. The Contractor shall provide travel invoice data on separate worksheets in Microsoft Excel spreadsheet format with the following details. Identify all cumulative travel costs billed by CLIN. The current invoice period's travel detail shall include separate columns and totals and include the following:

a. Travel Authorization Number/Identifier
b. Current invoice period
c. Names of persons traveling
d. Number of travel days
e. Dates of travel
f. Location of travel
g. Number of days per diem charged
h. Per diem rate used
i. Total per diem charged
j. Transportation costs

k. Total charges

ODCs and Incidentals

Cost incurred for ODCs and incidentals shall be shown on the monthly invoice and be itemized. The Contractor shall provide ODC/Incidental invoice data on separate worksheets in Microsoft Excel spreadsheet form with the following detailed information, as applicable.

a. Option Letter Identifying Number / Unique identifier
b. ODC/Incidental costs incurred
c. Description, make, model, and manufacturer part number of the ODCs/incidentals with itemized quantities, unit prices and extended prices
d. Warranty /maintenance coverage performance periods
e. Ship To Location(s) and Date(s) accepted by the Government
f. Current costs billed and Cumulative totals by CLIN/subCLIN level

Indirect and Material Handling Rate

Travel, ODCs, and incidentals incurred may be burdened with the Contractor's indirect/material handling rate consistent with the Contractor's proposal. Any proposed indirect or material handling rates proposed and invoiced shall be consistent with the Contractor's most recent Defense Contract Audit Agency (DCAA) rate approval or provisional rate letter. Offerors are advised that they will not be permitted to apply a burden rate of any kind to travel, ODCs, or incidental costs after award except to the extent that application of such burden is consistent with their proposal.

Charges:

- All invoice charges must be task item specific (only one task item) unless concurrent task item periods of performance exist.
- For invoices with concurrent task item periods of performance all invoice charges must be service month specific (that is one service month only).

Credits:

- If the credit invoice is for the same year of a particular ACT#, the contractor shall include that credit on a subsequent invoice submission against that same ACT#. If the contractor is unwilling to offset a subsequent invoice then they must submit a refund check.
- When the credit invoice is for a different year, the contractor shall submit a refund check for that credit invoice.

Invoices that net to a credit balance **SHALL NOT** be accepted. Instead a refund check must be submitted by the contractor to GSA accordingly. The refund check shall cite the ACT Number and the period to which the credit pertains. The contractor shall provide the credit invoice as backup documentation. Do not attach credit invoice in ITSS or on the Finance website. It must be attached to the refund check. The refund check shall be mailed to:

General Services Administration
Finance Division
P.O. Box 71365
Philadelphia, PA 19176-1365

Posting Acceptance Documents: Invoices shall be submitted monthly through GSA's electronic Web-Based Order Processing System, currently ITSS to allow the client and GSA COR to electronically accept and certify services received by the customer representative (CR). Included with the invoice will be all back-up documentation required such as, but not limited to, travel authorizations and training authorizations (including invoices for such).

Receiving Agency's Acceptance: The receiving agency has the following option in accepting and certifying services:

a. Electronically: The client agency may accept and certify services electronically via GSA's electronic Web-Based Order Processing System, currently ITSS, by accepting the Acceptance Document generated by the contractor. Electronic acceptance of the invoice by the CR is considered concurrence and acceptance of services.

Content of Invoice: The contractor's invoice will be submitted monthly for work performed the prior month. The contractor may invoice only for the hours, travel and unique services ordered by GSA and actually used in direct support of the client representative's project. The invoice shall be submitted on official letterhead and shall include the following information at a minimum.

1. GSA Contract Number
2. Contract ACT Number
3. Remittance Address
4. Period of Performance for Billing Period
5. Point of Contact and Phone Number
6. Invoice Amount
7. Skill Level Name and Associated Skill Level Number
8. Actual Hours Worked During the Billing Period
9. Travel Itemized by Individual and Trip (if applicable)
10. Training Itemized by Individual and Purpose (if applicable)
11. Support Items Itemized by Specific Item and Amount (if applicable)

All cost presentations provided by the Contractor shall include general and administrative charges, material handling, fees, and overhead applied consistent with the Contractor's approved price proposal and consistent with DCAA recommendations.

All invoice data shall be reported by CLIN and shall be further subdivided to lower level elements (subCLINs and ITSS Task Items) as directed by the Government to permit tracking and reporting of fund expenditures and appropriation data consistent with the requirements of DMDC and DMDC client agencies receiving support under this Task Order. The Contractor shall provide the invoice data in an editable Microsoft Excel spreadsheet using a format reviewed and approved by the Government. The Government reserves the right to modify invoicing requirements at its discretion. The Contractor shall comply with any revised invoicing requirements at no additional cost to the Government.

In the summary of the invoice, the contractor shall provide amounts billed by providing the following break out:

- For RAPIDS (CLIN X001):
 * CLIN X001A (baseline): $xx.xx
 * CLIN X001B (over and above components): $xx.xx
 * CLIN x006 (maintenance): $xx.xx
 * CLIN x010 (staffing logistics support): $xx.xx
 * CLIN X008a (travel): $xx.xx
 * CLIN X008b (non-travel ODCs): $xx.xx
GSA Alliant Fee

- For DBIDS (CLIN X002):
 * CLIN X002A (baseline): $xx.xx
 * CLIN X002B (over and above components): $xx.xx
* CLIN X002C (Site Surveys):
 * CLIN x006 (maintenance): $xx.xx
 * CLIN x010 (staffing logistics support): $xx.xx
 * CLIN X008a (travel): $xx.xx
 * CLIN X008b (non-travel ODCs): $xx.xx
GSA Alliant Fee

- For NTS/ETAS (CLIN X003):

 * CLIN X003A (baseline): $xx.xx
 * CLIN X003B (NTS training): $xx.xx
 * CLIN x006 (maintenance): $xx.xx
 * CLIN x010 (staffing logistics support): $xx.xx
 * CLIN X008a (travel): $xx.xx
 * CLIN X008b (non-travel ODCs): $xx.xx
GSA Alliant Fee

- For JAMMS (CLIN X004):

 * CLIN X004A (baseline): $xx.xx
 * CLIN X004B (over and above components): $xx.xx
 * CLIN x006 (maintenance): $xx.xx
 * CLIN x010 (staffing logistics support): $xx.xx
 * CLIN X008a (travel): $xx.xx
 * CLIN X008b (non-travel ODCs): $xx.xx
GSA Alliant Fee

Breakout = In each option letter exercised for CLIN X200, DMDC will provide the contractor with a summary of the number of components exercised, a list of each customer being supported, and a list of how many components are exercised for each customer. In return, for each DMDC customer being supported, the contractor shall provide to DMDC in each invoice a list of Site IDs that supported that customer in the invoiced month and each Action Item Number that was used to perform support. The contractor shall also provide the dollar amount of what the per

customer support cost was for the specific month and a running cumulative amount of dollars spent for each customer for the performance period.

Hardware/Software Invoicing:
If the entire Action Item (AI) is received in one invoicing cycle, the AI shall be invoiced at its' full value. If the AI is received across multiple invoicing cycles, the Contractor shall invoice AI expense incrementally after acceptance of the Government until the entire AI is delivered. At that time of fulfillment, the Contractor shall invoice the remaining value of the AI as contractually agreed to, with the reduction of all invoicing that has previously been submitted.

Final Invoice: Invoices for final payment must be so identified and submitted within 60 days from task completion and no further charges are to be billed. A copy of the written acceptance of task completion must be attached to final invoices. The contractor shall request from GSA an extension for final invoices that may exceed the 60-day time frame.

The Government reserves the right to require certification by a GSA COR before payment is processed, *if necessary*.

Close-out Procedures.
General: The contractor shall submit a final invoice within sixty (60) calendar days after the end of the Performance Period. After the final invoice has been paid the contractor shall furnish a completed and signed Release of Claims (GSA Form 1142) to the Contracting Officer. This release of claims is due within fifteen (15) calendar days of final payment.

8.0 CONTRACT ADMINISTRATION DATA

8.1 Contract Type: This is a hybrid Firm Fixed Price/ Time and Materials type task order. Core DMDC Requirements are Firm Fixed Price on a monthly basis. Optional DMDC Requirements are Fixed Price per component system. Optional tasks under 4.8 may be issued on Time and Materials basis if the Government is unable to definitize as Firm Fixed Price at time of issue.

8.2 Period of Performance: The base period of performance for this Task Order will be a one year base period from the date of award with four (4) 12-month option periods. The Government shall have the unilateral right to exercise the options at its own discretion.

8.3 Place of Performance:

a. The place of performance should be at the Contractor's facility. The location shall be proposed by the Contractor. All tasks performed under this Task Order are worldwide in nature with the exception of Task 4.3, "OCONUS Support", where the support is only required OCONUS.

b. Over the course of the Task Order, it is anticipated that operational needs may require technical expertise on site. Currently, DMDC has offices at the following locations:
   (1) Defense Manpower Data Center
   Monterey Bay Center

400 Gigling Rd
Seaside, CA 93955-6771

(2) Defense Manpower Data Center
Mark Center Facility
4800 Mark Center Drive
Alexandria, VA 22350

(3) DMDC Support Center - Europe
Bldg 214, Room 204
Sembach Kaserne
67681 Sembach-Heuberg DE

(4) DMDC/DBIDS Support Team - Southwest Asia
CRSP Zone 1, Building 314, Camp Arifjan
APO AE 09366

(5) DMDC Support Center Asia
Camp Humphrey's Army Garrison
Bldg S484, 2nd Flood
Pyeongtaek, South Korea 17709

c. At award, DMDC will require technical expertise on site at some DMDC OCONUS facilities. The contractor is also cautioned that there are space limitations at the Government facilities. Specifically, the individuals supporting Task 4.3.3 "Database Management and Support" and Task 4.3.4 "System Management and Support" shall be located at the OCONUS locations listed below. Likewise for OCONUS, the Government anticipates that at least initially during phase in, those personnel performing the duties in Section 4.3.2 will need to be located at our Government-provided locations. This support and availability of Government space may change over the life of the Task Order. Locations where support of Task 4.3.3 and/or Task 4.3.4 may be expanded in out years to cover other overseas locations if mission needs require that.

(1) DMDC Support Center - Europe
Bldg 214, Room 204
Sembach Kaserne
67681 Sembach-Heuberg

(2) DMDC/DBIDS Support Team - Southwest Asia
CRSP Zone 1, Building 314, Camp Arifjan
APO AE 09366

Note: Due to the length of time required to secure a visa for entry into Saudi Arabia, the Contractor shall provide and maintain a multi-entry visa for Saudi Arabia for at least one team member located in Southwest Asia so that on-site support can be provided on short notice to users of DMDC programs.

(3) DMDC Support Center Asia
Yongsan Army Garrison
Bldg S5450
Seoul, South Korea 140-766

8.4 Hours of Operation:
The core hours of operation shall be 08:00-17:00 local time, Monday through Friday (excluding Federal holidays), for the technical services staff; however, hours of operation will be driven by end user and mission requirements. The maintenance helpdesk shall be available 24x7x365.

8.5 Other Direct Costs (ODCs)
The Government will require the Contractor to incur ODCs resultant to performance under this task order. The Contractor shall furnish the COTS hardware and software materials and shipping to support DMDC projects during peacetime and during times of mobilization and/or contingency operations. The contractor shall be prepared to provide hardware, software, and shipping to support tasks worldwide. Such requirements shall be identified at the time of award is issued or may be identified during the course of performance, by the Government or the Contractor, reimbursement shall be made as specified in the task order.

Non-Travel ODC items (including tools) having a total procurement cost over $3,500 shall have the written approval of the Client Representative and the Contracting Officer prior to procurement. Federal contracting laws and regulations apply to all Contractor open market purchases of materials and equipment under this task. Prices must be determined fair and reasonable from competitive sources and are subject to Government audit. The Contractor shall maintain records documenting competitive sourcing, in strict compliance with the competition requirements set forth in the Federal Acquisition Regulation (FAR), for all material and ODC purchases. The Contractor shall provide copies of all such documentation upon request from the Government to verify that the Contractor complied with the competition requirements set forth in the FAR. Within the Contractor's price quote, any such rate shall be identified along with the DCAA point of contact (name, address, phone #, and email address) for rate verification. The Contractor shall only be allowed to apply indirect rates to ODC costs after award if such application is consistent with their successful price proposal and DCAA recommendations. No profit or fee shall be allowed on ODC costs.

All ODC items/ purchased by the Contractor for the use or ownership of the Federal Government shall become property of the Federal Government. If the Contractor acquires hardware/software maintenance support, all licenses and/or contractual rights to receive title shall be turned over to the Government upon completion of the task order. The Government's liability to reimburse the Contractor for costs incurred from the acquisition of hardware/software maintenance support shall be limited to costs incurred during the period of the order for which the Government received the said hardware/software maintenance support acquired by the Contractor on a cost reimbursable basis.

For all the procured ODCs, the Contractor shall receive in writing all the specifications and descriptions before actually procuring the items.

8.6 Shipping Instructions

8.6.1 Packaging/Packing/Shipping Instructions.

8.6.2 The prices for all COTS hardware and software Contract Line Item Numbers (CLINs) shall include packing and shipping worldwide. Ship all items when ordered to the location(s) indicated by the Government at the time of the order. Provide packaging and shipping to move equipment between locations as required.

8.6.3 All items to be delivered shall be packaged and marked to prevent deterioration and damage during shipping, handling, and storage to ensure safe arrival at the destination. All containers per shipment shall be clearly marked as follows:

(1) Name of Contract and Contract/Project/Task Number.
(2) Description/List of Items Contained in Shipment.
(3) Contractor's Name and Address.
(4) Contractor's POC and Phone Number to notify of any discrepancies between the contents and packing list.

8.6.4 Each shall be marked as package "x of y", where "x" is the package number and "y" is the total number of packages in the shipment. Bundling of equipment into single pallets may be used, where possible, as the vehicle of delivery. Use of this method of shipment will assist in keeping equipment together during shipment and verification/processing of systems once at the site. Contact the site to determine if use of pallets is acceptable and use the flag in the DMDC Configuration Management System, indicating whether or not each site can accept pallets (See Section 4.5.4). Sites unable to accommodate pallets have been identified, so that individual item shipment arrangements can be made.

8.6.5 In order to locate/track shipments that are lost or not delivered, the following shipping information shall be maintained by the contractor.

(1)Shipping Company (i.e., FedEx, UPS, USPS), Shipping Method Used (i.e., Overnight, 2 Day, 1st Class), and Tracking Number
(2) Shipping Destination Address (Street Address, City, State, Zip Code) and Addressee
(3) Number of Packages in Shipment
(4) Description/List of Items Contained in Shipment

8.6.6 Government Shipping Account Usage Reports: In limited cases, such as shipment of CAC consumables in OCONUS theaters, the Government authorizes the use of a DMDC shipping account. Tracking logs and monthly reporting will be required to report any authorized shipments.

8.7 Travel

Local or long-distance travel may be required to various locations CONUS and OCONUS, as directed by the Government on a cost-reimbursable basis in accordance with the Joint Travel Regulations (JTR) Standardized Regulations per FAR 31.205-46, Travel Costs. Before

contractor travel is executed, authorization must be given by the COR. See Appendix O, "Contractor Travel Authorization Form" and Appendix O.1, Travel SOP.

All non-local travel must be pre-approved by the Government and must be in accordance with the applicable Government Travel Regulation.

Note: Specific travel destinations cannot be determined at this time. Travel will be performed at the direction of the Government on a not to exceed basis. Any unused travel amount for the current period of performance will **NOT** be carried over to the next period of performance. If travel costs are expected to exceed this amount, the contractor shall notify the Contracting Officer's Representative (COR) and obtain written authorization from the GSA Contracting Officer prior to travel.

Costs for transportation may be based upon mileage rates, actual costs incurred, or a combination thereof, provided the method used results in a reasonable charge. Travel costs will be considered reasonable and allowable only to the extent that they do not exceed on a daily basis, the maximum per diem rates in effect at the time of the travel.

8.8 Kick-Off Meeting: The contractor shall not commence performance on the tasks assigned pursuant to this Performance Work Statement until the Contracting Officer (CO) or Contracting Officer Representative (COR) has conducted a kick-off or otherwise authorized by the GSA Contracting Officer. The kick off meeting shall be conducted within five business days of award of this Task Order.

8.9 Points of Contact:

DMDC COR
Mr. Rich Kalka
Defense Manpower Data Center
Enterprise Business Management, Acquisition Division
4800 Mark Center Drive, RM 04E25
Alexandria VA, 22350-6000
E-mail: Richard.w.Kalka.Civ@Mail.Mil
Tel: 210-308-1946

GSA Contracting Officer (CO)
Ms. Angela Bennert
GSA-FAS, Mid-Atlantic Region
The Dow Building - 3rd Floor
100 S. Independence Mall West
Philadelphia, PA 19106
E-mail: Angela.Bennert@gsa.gov
Tel: 215-446-5818

GSA Contract Specialist (CS)
Mr. Anthony Giannopoulos
GSA-FAS, Mid-Atlantic Region
The Dow Building - 3rd Floor

100 S. Independence Mall West
Philadelphia, PA 19106
E-mail: anthony.giannopoulos@gsa.gov
Tel: 215-606-1761

GSA Contracting Officer's Representative (COR)
Mr. Ruslan Gorbonos
GSA-FAS, Mid-Atlantic Region
The Dow Building - 3rd Floor
100 S. Independence Mall West
Philadelphia, PA 19106
E-mail: Ruslan.Gorbonos@gsa.gov
Tel: 215-446-5820

8.10 Key Personnel

8.10.1 Key Positions:

The contractor shall propose key personnel for the following functions:

a. OCONUS Installation Leads
b. CONUS Installation Leads
c. Communications Engineering Leads

The Contractor may propose additional key positions in addition to the functions listed above.

8.10.2 The Contractor is expected to minimize employee turnover with respect to personnel performing under this Task Order. The Contractor shall not remove or replace any personnel designated as key personnel under this TO without the written concurrence of the CO. Prior to utilizing other than personnel specified in the proposal submitted in response to this requirement, the Contractor shall notify the Government CO and the COR. This notification shall be no later than ten (10) calendar days in advance of any proposed substitution and shall include a resume for the proposed substitution and justification in sufficient detail to permit evaluation of the impact of the change on TO performance.

The request shall be written and provide a detailed explanation of the circumstances necessitating the proposed substitution. The Contractor shall submit a resume for the proposed substitute and any other information requested by the COR needed to approve or disapprove the substitution. The COR will evaluate such requests and promptly. The replacement key personnel shall possess skills of equal or greater qualifications to those being replaced. The CO will notify the Contractor of approval or disapproval thereof in writing.

If the Government CO and the COR determine that the proposed substitute personnel is unacceptable, or that the reduction of effort would be so substantial as to impair the successful performance of the work under the TO, the substitution will be denied and the Contractor shall propose an alternate candidate.

The Government will request an equitable adjustment for any key personnel positions left vacant for more than 14 calendar days.

8.11 Transfer of Hardware/Software Maintenance Agreements to follow-on contractors
The contractor shall ensure that all hardware/software agreements entered into under this task order are transferable to the Government and/or to other contractors at the discretion of the Government.

9.0 GOVERNMENT FURNISHED ITEMS

The Government will provide certain Government Furnished Property (GFP), Government Furnished Equipment (GFE), and Government Furnished Information (GFI) as stated in this PWS. The Government will allow remote access from the contractor's solution to DMDC assets required to support requirements stated in this PWS. For personnel located at the OCONUS Government facilities standard office equipment, communications services and office supplies will be provided.

9.1 Government Furnished Equipment.

The Contractor shall safeguard all Government Furnished Equipment (GFE) and shall designate a primary and alternate custodian to receive and account for all GFE. An initial inventory will be provided to the contractor by the DMDC upon initial GFE delivery to the contractor after award (example of which may be found on Appendix V). GFE shall be tracked by the contractor through applicable procedures in accordance with the FAR and DoD policy while in the contractor's possession. GFE in the contractor's possession shall be accounted for tracking purposes by serial number, description and location. At the end of this contract, the contractor shall return all GFE to the DMDC unless the DMDC instructs otherwise. The contractor shall recognize this responsibility and liability for, and warrant the safekeeping of GFE provided to them.

The Government property shall be used only for performing this Task Order, unless otherwise provided in this Task Order or approved by DMDC.

Any GFE that the Government approves to be excessed from the contractor's storage/possession shall be accomplished in accordance with established Government procedures. The Contractor shall prepare all required documentation necessary for disposal and provide copies to DMDC as required.

It should be noted that the contingency systems listed in PWS 4.1.8.1 will be provided to the Contractor as GFE.

9.2 Government Furnished Information (GFI)

The following information will be provided by the Government to the contractor:

a. Published material and documentation associated with the various DMDC applications hardware and software.

b. The latest DMDC applications' installation compact disks – read only memory (CD-ROMs)/Digital Video Disks (DVDs), IAVA patches/updates, and installation/configuration instructions.
c. The latest DMDC application site and system configuration database.
d. The latest DMDC configuration management baseline data (currently maintained with SQL*Server).
e. The latest supported DMDC applications' installation and software release schedule information.
f. Current documentation including architecture and network drawings, etc.

9.3 Government Furnished Training.

9.3.1 The Contractor shall attend all government provided training or application certification tests as applicable to their support role for applications/systems or for access to government networks/systems that contractor personnel may be required to have access to. For example, DSC personnel in Europe and Asia are currently required to complete Army classes in order to use the local Army network. Additionally, training may include security or privacy training. Another example is personnel entering a secure shipyard are required to take training prior to being given access to the ships. Training unique to, or required by, DMDC may be provided by DMDC and contractors may attend at the discretion of DMDC.

9.3.2 The Contractor shall maintain current knowledge on applicable DMDC applications. Ongoing, periodic on-site refresher training will be available as agreed to by the contractor and DMDC. Additional training requirements and the estimated average completion time are provided at Appendix P, "Learning Site Course List".

10.0 SECURITY

10.1 The following security levels are required:

- Level I for user accounts (SSM or VO)
- Level II for IT personnel who have privilege accounts higher than RAPIDS users (access to RAPIDS servers for example)
- Level III for only for IT personnel who have domain access (domain controllers, local servers accounts)

10.2 The Contractor shall establish network connectivity to DMDC to accomplish the tasks in this PWS. The facility must be accredited to the appropriate security level as part of the overall certified facility infrastructure and must be in place 90 days from date of contract award.

10.3 The Contractor shall provide a solution which includes Non-Secure Internet Protocol Router Network (NIPRNet) connectivity, or a Virtual Private Network (VPN) or an encrypted point–to-point technology. The Point to Point circuit end-point would terminate at Seaside, CA and/or Auburn Hills, MI. The government network domain must be securely maintained in a separate environment from any commercial domains at the contractor site. The connectivity solution(s) must support both the end users as well as the contractor support personnel.

10.4 The Contractor and all Contractor personnel with access to or responsibility for nonpublic Government data under this contract shall comply with DoD Directive 8500.1 Cybersecurity, DoD Instruction 8510.01 Risk Management Framework, DoD Directive 5400.11 DoD Privacy Program, DoD 6025.18-R DoD Health Information Privacy Regulation, DoD 5200.2-R Personnel Security Program, and Homeland Security Presidential Directive (HSPD) 12.

10.5 The Contractor shall establish appropriate administrative, technical, and physical safeguards to protect any and all nonpublic Government data to ensure the confidentiality, integrity, and availability of government data. At a minimum, this must include compliance with DoDD 8500.1 and DoDI 8500.2 and provisions for personnel security and the protection of sensitive information, including Personally Identifiable Information (PII).

10.6 The Contractor shall ensure all media containing sensitive information (e.g., hard drives, removable disk drives, CDs, DVDs) considered for disposal are destroyed. Prior to destruction, media will be sanitized, i.e., all prudent and necessary measures shall be taken to ensure data cannot be retrieved through known conventional or unconventional means.

10.7 The Contractor systems and information networks that receive, transmit, store, or process nonpublic government data must be accredited according to DoDI 8510.01 RFM)and comply with annual Federal Information Security Management Act (FISMA) security control testing. All systems subject to RFM must present evidence of Assessment and Authorization (A&A) testing in the form System Identification Profile (SIP), RFM Implementation Plan (DIP), RFM Scorecard and Plan of Action and Milestones (POA&M). Evidence of FISMA compliance must be presented in the form of a POA&M. The Contractor will be responsible for the cost of IA A&A and FISMA testing required for any Contractor owned and operated network, facility and/or application processing DoD information.

10.8 Personnel Security Clearance and Vetting Requirements.

All personnel shall have appropriate clearances at the time of the award.

10.8.1 Prior to beginning work, all contractor personnel shall comply with DMDC contractor vetting requirements (see Appendix Q, “Contractor Vetting DMDC Form-85R”) for submittal of Information Technology (IT) trustworthiness determination requirements and ensure that all personnel are designated as IT-I, IT-II, or IT-III as determined by DMDC according to the criteria of the position sensitivity designation (DODI 5200.2-R). For positions involving access to classified information, the appropriate Secret or Top Secret clearance will be required as needed.

10.8.2 Contractor personnel with access to DoD non-public Government data shall comply with HSPD-12 Personal Identity Verification (PIV) issuance requirements, known as the Common Access Card (CAC) for DMDC.

10.8.3 The Contractor personnel shall be CAC ready prior to reporting for work. All Contractor personnel shall obtain/maintain a favorable FBI National Criminal History Check (fingerprint

check), two forms of identity proofed identification (I-9 document), and submit a National Agency Check and Law Credit (NACLAC) vetting package for processing.

10.8.4 The Contractor shall comply with DMDC Information Systems Security Group (DISSG) procedures (standard operating procedures will be released to the contractor at the time of award) for Requirements to Access DMDC Resources to maintain proper security clearance or vetting prior to beginning work under the contract. Due to varying access requirements, information and data to which each contractor person may have access, personnel security clearance and vetting requirements will vary.

10.8.5 The Contractor shall comply with the government provisioning procedures for all personnel accessing the DMDC networks, applications and databases. First, the contractor will submit a DMDC form 85R (see Appendix Q, "Contractor Vetting DMDC Form-85R") for each person so the government can determine the IT level of access required for their position. (see section 8.3.1). Next, the personnel will have to meet the certification requirements for any applications used to view or update data, for example RAPIDS and JPAS. The third step requires the contractor personnel to be provisioned for each application they have to use either in read or update mode.

10.8.6 U.S. citizenship is required for all personnel who have not previously submitted trustworthiness determination and/or security clearance by October 26, 2006.

10.8.7 If at any time, any Contractor person requiring a CAC is unable to obtain/maintain an adjudicated NACLAC, the Contractor shall immediately notify the DMDC Information Systems Security Group (DISSG) and remove such person from work under this contract and the government site if applicable. If at any time, any contractor person is unable to maintain a security clearance the DISSG shall be notified immediately and the contractor person shall be immediately removed from work under this contract and the government site if applicable.

10.8.8 The Contractor shall execute Non-Disclosure Agreements prior to being provided access to any DMDC application or administrator passwords. The contractor should refer to DoD Regulation 5200.2-R, Personnel Security Program for details.

10.8.9 The Contractor shall display the Government-issued access badges (CAC) when accessing Government facilities.

10.8.10 The Contractor shall execute a DD Form 2841, Department of Defense (DoD) Public Key Infrastructure (PKI) Certificate of Acceptance and Acknowledgement of Responsibilities, and adhere to the acknowledged responsibilities there under (required for CAC issuance).

10.8.11 The Contractor shall comply with the following data access requirements:

10.8.12 Vetting at the appropriate designated level; Completion of DMDC Information Assurance/Security Awareness training (annually); Completion of DMDC Privacy Awareness Training; Execution of the DMDC User Agreement; and Other security related training provided by DMDC to ensure users understands all DMDC and DoD protocols. The Contractor shall

Complete contractor security vetting using Appendix Q as a template.

10.9 The contractor facility and infrastructure shall operate according to the DOD Information Assurance Assessment and Authorization Process (RFM) policies or National Institute of Standards and Technology (NIST) 800-53 to ensure the integrity and security for accessing, storing and transporting of DMDC data. Additionally, the facility for hardware and software asset management shall meet the NIST 800-171 Rev 1 or higher requirements for quality management.

11.0 STATUS OF FORCES AGREEMENT (SOFA) STATUS OF THEATHER BUSINESS CLEARANCE

The contractor shall comply with Host Nation and US Government requirements to obtain SOFA Status, Technical Expert (TE) or Analytical Support (AS)Accreditation, or Theater Business Clearance (TBC) for all contractors assigned OCONUS in accordance with US Forces Korea (USFK) Regulation 700-19, Army in Europe (AER 715-9), or U.S Central Command Contracting Command Guidance. The host nation government makes the final determination for approval. Generally speaking, qualifications are U.S. citizenship and varying amounts of technical expertise. Extension of DoD-provided benefits and privileges is dependent upon SOFA status determination. Benefits and privileges include reimbursable health care, commissary, exchange, and limited access to furnishings and appliances if these are available through the local installation. The Government will facilitate the SOFA process to request SOFA status accreditation as Technical Expert (TE) or Analytical Support (AS) contractors. TE/AS status is determined by the Host Nation Government. If non-TE/AS personnel are hired, they must be US citizens and the contractor is responsible for obtaining any required work or residence permits required by the Host Nation. The Government will facilitate TBC requests upon notification of contractors that require TBC.

12.0 CERTIFICATION OF CONTRACTOR EMPLOYEES

The contractor shall ensure the certification compliance IAW DoD 8140.01 Cyberspace Workforce Management. The contractor personnel shall agree as a "condition of employment" to obtain the appropriate baseline certification upon contract award. The contractor shall ensure that all TIER I/TIER II support personnel obtain and maintain certification corresponding to Information Assurance Technical Level I (IAT I). Contractor employees performing functions as Application Support are required to obtain and maintain certification corresponding to Information Assurance Technical Level II (IAT II). Contractor employees performing functions as Systems administrators/Enterprise Management are required to obtain and maintain certification corresponding to Information Assurance Technical Level II (IAT II). Contractor employees performing functions as Network Technicians are required to obtain and maintain certification corresponding to Information Assurance Technical Level III (IAT III). Contractor employees performing functions as Engineers are required to obtain and maintain certification corresponding to Information Assurance Technical Level III (IAT III). Contractor employees performing functions as Network Security Technicians are required to obtain and maintain certification corresponding to Information Assurance Technical Level III (IAT III). The contractor shall ensure all employees meet the minimum requirements within six months of the

task order award. Further, the contractor shall ensure all new hires meet the minimum requirements for their respective positions upon initiation of their duties. Contractor Technical Level I, II and III personnel must also obtain the appropriate computing environment certification/s required by their employing organization. The contractor shall be responsible for yearly maintenance fees to keep these certifications. This includes but is not limited to 120 Continuing Professional Education credits (CPEs) every three years.

13.0 ORGANIZATIONAL CONFLIC OF INTEREST

The Contractor and subcontractor personnel performing work under this contract may receive, have access to, or participate in the development of proprietary or source selection information (e.g., cost or pricing information, budget information or analyses, specifications or work statements, etc.), or perform evaluation services which may create a current or subsequent Organizational Conflict of Interests (OCI) as defined in FAR Subpart 9.5. The Contractor shall notify the Contracting Officer immediately whenever it becomes aware that such access or participation may result in any actual or potential OCI and shall promptly submit a plan to the Contracting Officer to avoid or mitigate any such OCI. The Contractor's mitigation plan will be determined to be acceptable solely at the discretion of the Contracting Officer and in the event the Contracting Officer unilaterally determines that any such OCI cannot be satisfactorily avoided or mitigated, the Contracting Officer may effect other remedies as he or she deems necessary, including prohibiting the Contractor from participation in subsequent contracted requirements which may be affected by the OCI. The OCI document is provided as Attachment B and shall be submitted with the proposal

14.0 APPLICABLE DOCUMENTS

- Army in Europe Regulation (AER) 715-9, Contractor Personnel in Germany- Technical Expert, Troop Care, and Analytical Support Personnel;
- DoD Instruction (DoDI) 5000.64, Accountability and Management of DoD Equipment and Other Accountable Property;
- DoD Directive 5200.02-R Procedures for the DoD Personnel Security Program;
- DoD Directive 5200.08-R, DoD Physical Security Program;
- DoD Directive 5400.11 DoD Privacy Program;
- DoD 5400.11-R DoD Privacy Program;
- DoD Directive 6025.18-R, DoD Health Information Privacy Regulation;
- DoD Directive 8140.01, Cyberspace Workforce Management;
- DoD Directive 8500.01, Cybersecurity;
- DoD Directive 8510.01 Risk Management Framework (RMF);
- Homeland Security Presidential Directive (HSPD)12;
- US Forces Korea (USFK) Regulation 700-19, The Invited Contractor and Technical Representative Program.

15.0 LIST OF PWS APPENDICES

See UCF Section J for the list of Appendices included in this PWS.

16.0 SECTION 508 COMPLIANCE REQUIREMENTS

The contractor shall support the Government in its compliance with Section 508 through-out the development and implementation of the work to be performed. Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d) requires that when Federal agencies develop, procure, maintain, or use electronic information technology, Federal employees with disabilities have access to and use of information and data that is comparable to the access and use by Federal employees who do not have disabilities, unless an undue burden would be imposed on the agency. Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal agency, have access to and use of information and data that is comparable to that provided to the public who are not individuals with disabilities, unless an undue burden would be imposed on the agency. Section 508 also requires that individuals with disabilities who are members of the public seeking information or services from the Federal Agency, have access to and use of information and data that is comparable to that provided to the pubic who are not individuals with disabilities, unless an undue burden would be imposed on the agency. The Offer shall review the following websites for additional 508 compliance information.

http://www.section508.gov/index.cfm?FuseAction=Content&id=12
http://www.access-board.gov/508.htm
http://www.w3.org/WAI/Resources